gTLD 目录服务

专家工作组

最终报告：

下一代

注册目录服务 (RDS)

本文档的来由状况

这是 gTLD 目录服务专家工作组 (EWG) 提交的最终报告，详细阐述了我们向 ICANN 理事会提出的用下一代注册目录服务 (RDS) 代替当前 WHOIS 系统的建议。

I. 执行摘要

本最终报告由 gTLD 目录服务专家工作组 (EWG) 编撰，详细阐述了我们向 ICANN 总裁/首席执行官和理事会提出的用下一代注册目录服务 (RDS) 代替当前 WHOIS 系统的建议。

本最终报告是历经 15 个多月紧张工作后的最终成果。在这期间，这个由志愿者组成的多元化小组投入了无数时间进行深入研究；参考了超过 2600 页的公众意见、调查回复和研究结果；参与了 19 场机构群体意见公开征询会、35 天的面对面 EWG 会议、42 场 EWG 电话会议、200 多场分组电话会议，以及与外部专家及机构群体成员召开了无数场意见收集会议。所有这一切都是为了探寻一个答案：

是否存在可以替代当前 WHOIS 系统以更好地服务于全球互联网群体的另一种方案？

答案是肯定的。EWG 一致建议，舍弃授予每位用户相同的完全匿名公共访问权来访问（往往不准确的）gTLD 注册数据的当前 WHOIS 模式。

同时，EWG 建议实行向下一代 RDS 转化的范式转换，确保 gTLD 注册数据的收集、验证和披露仅用于容许目的。

在 RDS 中，基本数据仍然保持对公众开放，其他数据则仅限经认证的请求者访问，这些请求者必须表明自己的身份、陈述自己的目的并同意合理使用相关数据。

接下来，我们将用超过 150 页的篇幅来阐述 EWG 在构思建议（关于采用新 RDS 的详细提案）和得出以下结论时所考虑的意见和开展的研究：

- 这一问题非常复杂。
- 为了确保拟议的 RDS 切实可行，EWG 从多个角度考虑了这个问题并开展了大量的研究。
- 尽管拟议的 RDS 并不完美，但它是 EWG 用心的结果，并且在各个本不应分割、相互依存的要素之间实现了平衡。
- 拟议 RDS 旨在用一种前所未有的方式，正面解决下列问题：
    - 数据隐私难题；
    - 长期损害数据质量和准确性的验证挑战；以及
    - 实现数据访问和问责制平衡。
- ICANN 应将 RDS 作为一个整体全盘接受。如只接受本报告建议的部分设计原则，将无法为整个生态系统带来最大益处。

本最终报告，包括其中提出的建议和下一代 RDS 原则，均反映了工作组成员的一致意见。值得注意的是，EWG 在编撰报告时采用了广泛的视角，且 EWG 成员中包括了相关的利益主体。[1]

EWG 相信，本最终报告定能达到 ICANN 理事会的指示要求，帮助重新定义 gTLD 注册数据的用途和披露，为 ICANN 机构群体（通过通用名称支持组织，GNSO）制定新的 gTLD 目录服务全球政策奠定坚实基础。

EWG 也相信，本最终报告中提出的 RDS 定能比当前系统提供更为坚实的基础，使 GNSO 能针对 gTLD 注册数据制定新的全球政策，不仅保护个人隐私，同时确保在未来几年提高整个 ICANN 生态系统的准确性、责任追究和透明度。

EWG 建议，理事会、GNSO 和 ICANN 机构群体在审议本最终报告时应该着眼于以下两个问题：

- RDS 是否优于当前的 WHOIS 系统？
- 如果否，ICANN 机构群体是否同意继续使用当前 WHOIS 系统，以及它能否满足不断发展的全球互联网的需求？

背景

EWG 是 ICANN 首席执行官 Fadi Chehadé 应 ICANN 理事会的要求组建的，旨在帮助打破 ICANN 机构群体内部关于如何替代当前 WHOIS 系统的持续了近十年之久的僵局。[2]

除了解决机构群体报告和研究中提到的诸多 WHOIS 缺陷以外[3]，EWG 的使命还包括重新审视并定义收集和维护 gTLD 注册数据的目的、考虑如何保护这些数据以及提出能更好满足全球互联网群体需求的下一代解决方案。

从零开始的 EWG 对关于注册数据的目的、使用、收集、维护和披露的基本假设提出了质疑。EWG 将 gTLD 目录服务中涉及的所有利益主体均纳入了考虑范围内，分析了他们对数据准确性、访问和隐私的需求。最终，EWG 认为可以通过其他方法来更有效地满足这些需求。

[1] 请参见附录 J 了解 EWG 的成员构成以及这些成员拥有的专业知识。

[2] 请参阅 https://www.icann.org/news/announcement-2-2012-12-14-en

[33] 请参阅附录 B 查看记录 WHOIS 缺陷的报告列表。

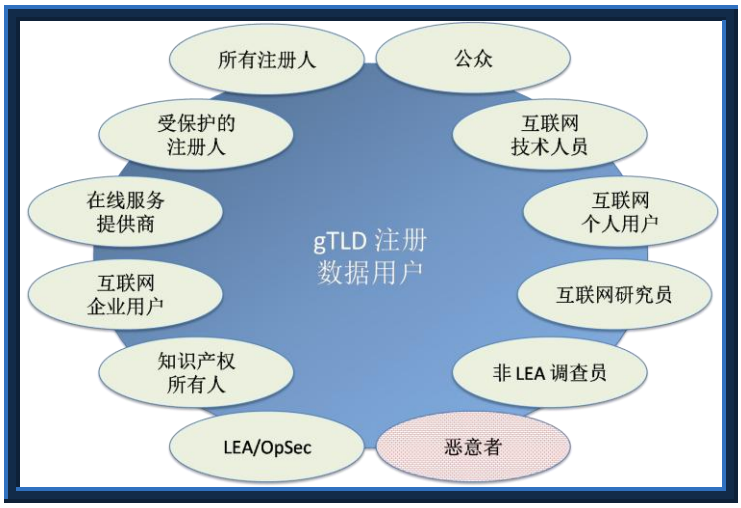
为了给审议工作提供依据，EWG 发表了一份高层目的声明，旨在使本报告的建议符合 ICANN 使命，以及设计一个满足以下要求的域名注册和维护支持系统：

- 提供适当访问准确、可靠且统一的注册数据的途径；
- 保护注册人信息的隐私；
- 启用能够识别、建立和维护联系注册人的能力的可靠机制；
- 支持可解决涉及注册人的诸多问题的框架，包括但不限于：消费者保护、网络犯罪调查和知识产权保护；以及
- 提供可满足适当执法需求的基础架构。

用户和目的

EWG 分析了收集和存储 gTLD 注册数据以及向广大用户提供这类数据的现有及潜在目的，同时分析了大量具有代表性的实际 WHOIS 使用案例。

为了整理出 RDS 必须涵盖的用户和容许目的，明确必须加以阻止的潜在滥用行为，EWG 考虑了这些使用案例的总体情况和从中获得的经验以及参考材料和机构群体意见。



需要满足或禁止的目的

EWG 依据自己的使命，对所有这些用户进行了核查，确定了现有工作流程和未来可能的工作流程，以及流程涉及的利益主体和数据。

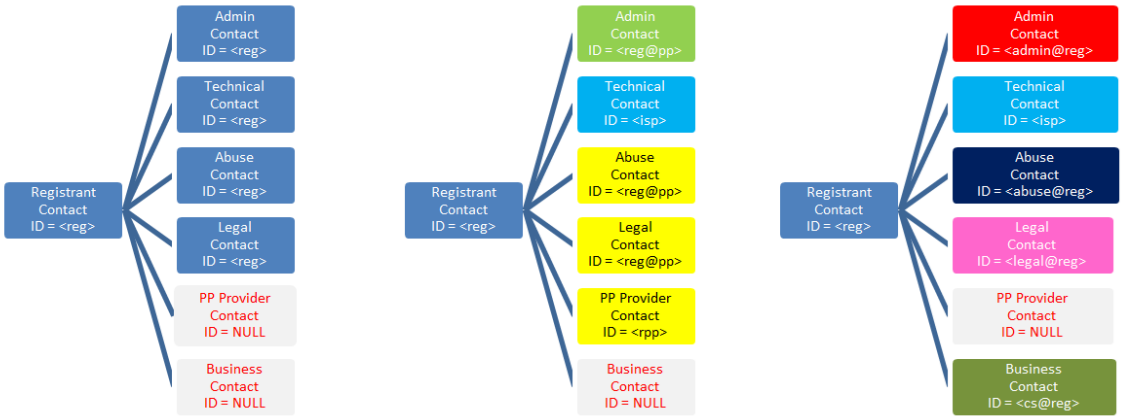
EWG 分析了域名注册信息需求，以明确强制性数据元素、相关风险、隐私法律和政策含义以及解决本报告中探讨的其他问题。EWG 建议的容许目的如右图所示。

以下为当前已确定的容许目的及相关注册数据、联系信息和查询需求，更多详细信息请参阅第 III 节。

目的	任务示例…
域名控制	创建、管理和监控注册人自己的域名，包括创建域名、更新域名信息、迁移域名、续用域名、删除域名、维护域名投资组合和检测是否有人对注册人自己的联系信息进行欺诈性使用。
个人数据保护	确定某一域名的经认证隐私/代理服务提供商或安全保护凭证批准方以报告滥用行为、请求披露或出于其他原因联系提供商。
解决技术问题	若要解决与域名使用相关的技术问题，包括电子邮件发送问题、DNS 解析失败和网站功能问题，需与负责处理此类问题的技术人员联系。
域名认证	在证书颁发机构 (CA) 向某一域名对应的主体签发 X.509 证书时，需要确认该域名确实注册在该证书主体名下。
个人互联网使用	明确使用域名的组织以培养消费者信任，或联系该组织以提交客户投诉或提交对该组织的投诉。
企业域名的购买或销售	域名购买查询、收购另一注册人的域名，以及开展尽职调查研究。
学术/公众利益 DNS 研究	针对 RDS 内所发布域名开展符合公众利益的学术研究，包括关于注册人和指定联系人的信息、域名的历史信息和状态以及注册在某一已知注册人名下的域名。

目的	任务示例…
法律诉讼	调查其他域名对注册人姓名或地址的潜在欺诈性使用、调查可能的商标侵权、在采取法律诉讼前联系注册人/被许可人的法律代表，并在问题无法得到圆满解决后采取法律诉讼。
监管和合同的执行	税务机构利用在线服务对企业进行调查、UDRP 调查、合同合规性调查以及注册数据托管审核。
犯罪调查和减少 DNS 滥用	向能够调查和解决滥用行为的人报告这类行为，或在离线犯罪调查期间联系与某一域名相关的实体。
DNS 透明度	查询注册人公布的注册数据以满足广大公众的知情需求。

为了让公众基于目的对注册数据进行访问，同时加强沟通和个人隐私保护，EWG 制定了一系列“基于目的的联系人”(PBC) 原则。在既定角色和职责的支持下，EWG 实现了 PBC 与所有需要进行联系的容许目的之间的关联。下图描绘了三个关联示例，更多详细信息请参见第 III 节和第 IV 节。



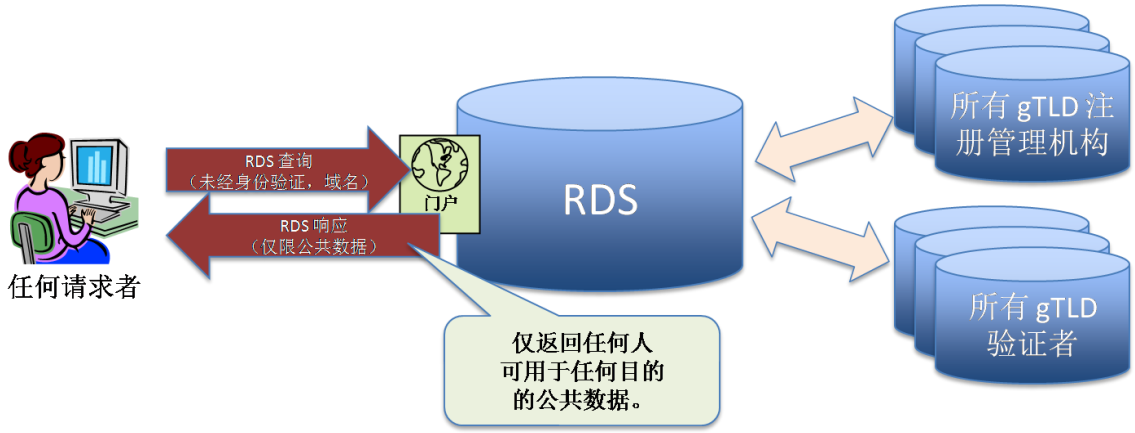
EWG 进一步分析了所有注册数据元素（从 2013 RAA 中定义的数据开始），得到了一系列用于数据收集和披露的指导原则，这些原则不仅与建议的 PBC 框架相吻合，还与为符合数据保护法而提出的建议相吻合。为了明确注册人和联系人可能选择公开哪些新的数据元素，进而提高沟通的可靠性，EWG 提出了进一步建议。详细的建议内容请参见第 IV 节，相关示例请参见附录 E。

目的导向访问

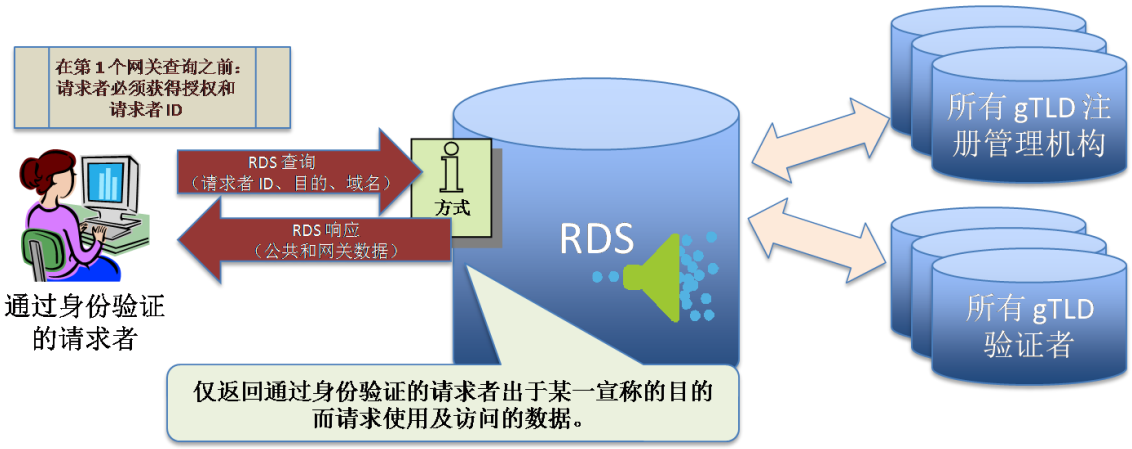
EWG 建议的 RDS 采取一切归零、从头开始的方式，舍弃当前“一刀切”的 WHOIS 系统，支持公众以目的为导向访问经验证的数据，以此加强隐私保护和问责制，提高准确性。EWG 相信，这种全新的访问模式定能通过以下途径，加强对所有涉及披露和使用 gTLD 域名注册数据的相关方的责任追究：

- 记录所有访问 gTLD 注册数据的行为（包括无需身份验证的公共数据元素访问），检测和减少滥用行为；
- 控制对较敏感数据元素的访问，仅在请求者申请接收 RDS 访问并通过认证时才向其开放这类数据，且开放程度对每位用户及其所述目的而言适当；以及
- 根据所有请求者明确同意的条款和条件审核公共数据访问和网关数据访问，最大限度减少滥用，并对不当使用行为给予处罚和采取其他补救措施。

关于 EWG 在就公共数据访问和网关数据访问提出详细建议时所依据的数据访问原则，请参见第 IV 节。如下图所示，无论是否通过身份验证，任何人均可以向 RDS 请求访问公共数据元素。



网关数据元素也可以通过 RDS 请求访问。不过，要访问这类数据，请求者必须先通过认证。随后，请求者可以出于已陈述的目的提交经过身份验证的数据元素查询请求。



更多关于返回的数据元素如何响应公共和网关数据查询请求、用户和目的如何决定网关访问以及 RDS 用户认证机构如何在授权和审查网关访问中发挥作用的详细说明，请参阅附录 E。

隐私和数据保护

EWG 的工作核心在于，研究如何设计一个既能提高所收集数据的准确性又能为那些寻求隐私保护和维护的注册人提供适当保护的系统。

EWG 认识到，个人信息受数据保护法的保护，而且即使没有这类法律，个人也有正当理由寻求对自己个人信息的严格保护。此外，部分企业和组织也可以正当目的为由寻求信息保护，例如当他们准备推出新产品系列时，或者针对小型企业用个人信息作为公司联系信息的情况。

鉴于此，EWG 提出了一系列相应建议，旨在确保日常的数据访问符合隐私法和数据保护法，详细的建议内容请参见第 VI 节。这些建议原则包括：

- 建立相应机制，确保日常访问符合数据保护相关法律要求，促进 RDS 生态系统内参与者之间的数据传输；
- 制定与隐私法和数据保护法统一的标准合同条款并将其写入政策中；
- 通过“规则引擎”应用数据保护法；以及
- 如何将 RDS 数据存储位置与执法机构访问进行关联。

除了数据保护法可提供的隐私保护，RDS 还建议在 RDS 生态系统中引入以下两条原则以满足隐私保护需求：

- 经认证的隐私/代理服务，供一般性使用；以及
- 经认证的安全保护凭证服务，供处于危险之中的人和在言论自由权可能不被承认或发言者可能遭受迫害的情况下使用。

EWG 进一步建议 ICANN 探讨制定单一、统一的隐私政策来全面监管 RDS 活动。

为了满足对可加强问责制的更统一、可靠隐私和代理服务的需求，EWG 在其 PBC 原则中纳入了隐私/代理通信。同时，在为 GNSO 隐私和代理服务认证问题工作组提供意见时，EWG 还建议采用隐私/代理原则和框架。

对于某些能证明自己如果在注册数据中暴露身份便会存在危险的个人和群体，为了满足他们的需求，EWG 建议应用安全保护凭证框架，这样，凭借证人和可信第三方在处于危险之中的实体与注册服务商之间建立起的屏障，相关方便可使用安全凭证匿名申请和接收所注册的域名。为此，EWG 建议 ICANN 设立独立的可信审查委员会，负责验证组织或个人的危险言论是否为真，并在证实后授予（以及在必要时撤销）相应凭证。

数据质量

EWG 建议对注册人数据采用极其严格的验证方式，要比当前 WHOIS 系统所提供的或可通过广泛实施 2013 RAA 加以改进的验证更为严格。具体的数据质量改进措施包括以下。

- 注册人应大大改进自己提供的以目的为导向的联系信息，使出于各种目的的请求者能根据这些信息联系到相应的联系人。采取激励措施，促使注册人提供准确的联系人信息。
- 控制对较敏感数据元素的访问，使注册人缺少提供错误数据的动机，加强对他们确保数据准确性的责任追究。

此外，EWG 还提出了两条相关但独立的改进措施：

- 标准验证：采用定期检查和收集时验证相结合的方式，对所有 gTLD 注册数据进行标准验证，还可以选择对联系人数据块进行预验证以便在多个域名注册中重复使用以及使 RDS 用户能够查看数据的上次验证时间和验证级别；以及
- 经预验证的联系人目录：该目录与域名目录存在概念上的区别，旨在提高数据元素的质量和可重用性以及防止对个人数据的欺诈性使用，其中，此处的数据元素是指用于联系域名注册人及其指定为 PBC（即可以出于与某一域名注册相关的各种目的与之取得联系）的个人或组织的数据。

关于详细阐述这些建议的原则的流程可参见第 V 节。

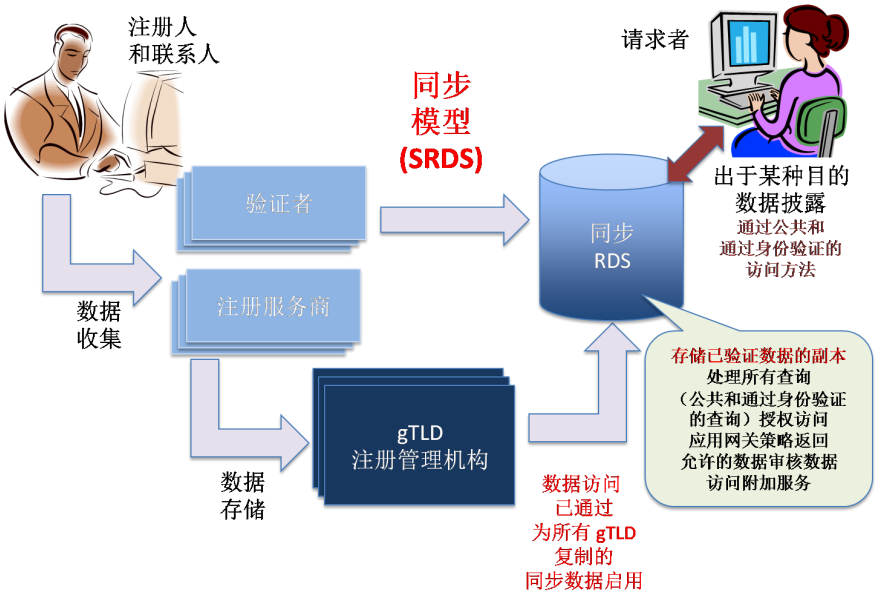
实施模式

在考虑如何将这些原则和建议付诸实践时，EWG 深入探究了多种备选的模式。所有模型均使用如附录 F 中所述的一组多角度标准进行了评估。在经过严格的分析后，EWG 得出了以下结论。

- 目前，注册服务商或注册服务商的附属机构从它们自己的客户（注册人）那里收集并存储注册信息。本质上，这是一个分布式流程。除了注册服务商或附属机构继续从注册人那里收集注册数据以外，EWG 还建议验证方收集联系数据。
- 适用于存储所有 gTLD 注册信息的模式不止一种。EWG 找到了多种可能的模式，并指出其中它认为最有发展潜力的两种，建议 ICANN 依据评估标准从这两种模式中二选一。
- 为了保护数据主体的隐私，必须构建一个集中化的接口，使适用请求者能够访问所有 gTLD 的注册信息，包括无需通过身份验证的公共数据访问和需要通过身份验证的网关数据访问。
- RDS 必须将 RDAP 或 EPP（根据每个接口酌情选择）用作底层目录访问协议，以便从存储位置获取注册信息（无论它位于什么位置）。

EWG 建立并测试了多种备选的系统模式（详细信息请参见附录 F），包括 ICANN 机构群体建议的模式。这些模式的区别在于是将注册信息复制到 RDS 中还是通过 RDS 查询注册信息。为了明确这些区别带来的影响，EWG 几乎对每种模式进行了测试。在对比了这些可能模式之后，EWG 发现，除了当前的 WHOIS 系统，其他所有模式都能在某种程度上满足 EWG 提出的 RDS 原则要求。其中，EWG 锁定了两种最具发展潜力的模式以待进一步研究，即联合模式和同步模式（曾被称为“集中式模式”）。

为了进一步为分析提供指导和数据，EWG 委托中立第三方 (IBM) 开展了一项“实施模式成本分析”，以确定这两种模式具有哪些要求以及潜在成本如何。在参考了 IBM 分析报告并进行了深入分析之后，EWG 发现联合模式对整个 RDS 生态系统而言的成本较高，因此，**EWG 最终建议采用同步 RDS (SRDS)。**



结语

鉴于最终报告篇幅较长、内容复杂且包含大量细节，本执行摘要无法一一概述，建议读者参阅本最终报告正文了解更多信息。

目前，EWG 已将本最终报告提交给 ICANN 首席执行官和理事会并在网上公开发布，在即将于 2014 年 6 月举行的 ICANN 伦敦会议期间，EWG 将针对本报告举行多场公众意见征询会。此外，EWG 还会通过网络会议和其他平台对报告进行探讨，同时回答 ICANN 机构群体提出的相关问题。本最终报告旨在为建立理事会要求的 GNSO 政策制定流程 (PDP) 创造基础，以在适当情况下制定 gTLD 注册数据提供政策和合同谈判政策。

EWG 相信，本最终报告定能达到 ICANN 理事会的指示要求，帮助重新定义 gTLD 注册数据的用途和披露，为 ICANN 机构群体（通过 GNSO）制定新的 gTLD 目录服务全球政策奠定坚实基础。

II. EWG 的使命、宗旨和成果

a. 使命

gTLD 目录服务专家工作组 (EWG) 是 ICANN 首席执行官 Fadi Chehadé 应 ICANN 理事会的要求组建的，旨在帮助打破 ICANN 机构群体内部关于如何替代当前 WHOIS 系统的持续了近十年之久的僵局。在这期间，机构群体发布了多份报告和研究[4]，指出当前系统中存在的诸多缺陷，并呼吁制定相应的解决方案。

EWG 的使命是重新审视并定义收集和维护 gTLD 目录服务的目的、考虑如何保护这些数据，以及提出能更好地满足全球互联网群体需求的下一代解决方案。该工作组从零开始，探索和质疑了关于注册数据的目的、使用、收集、维护和披露的基本假设。EWG 将 gTLD 目录服务中涉及的所有利益主体均纳入了考虑范围内，分析了他们对数据准确性、访问和隐私的需求，并研究了能够更有效满足这些需求的可能方法。

b. 目的

为了帮助指导 EWG 的审议工作，工作组发表了一份高层目的声明，作为检验其结论和建议是否符合目的的依据，声明内容如下：

> 为了帮助 ICANN 执行对全球互联网唯一标识符系统的协调使命，以及确保互联网唯一标识符系统稳定安全地运行，有必要收集 gTLD 域名信息，以提高所有利益主体对互联网的信任和信心。
>
> 因此，必须设计出能够满足以下要求的系统来支持域名注册和维护：
>
> - 提供适当访问准确、可靠且统一的注册数据的途径
> - 保护个人信息的隐私
> - 启用能够识别、建立和维护联系注册人的能力的可靠机制
> - 支持可解决涉及注册人的诸多问题的框架，包括但不限于：消费者保护、网络犯罪调查以及知识产权保护
> - 提供可满足适当执法需求的基础架构

[44] 请参阅附录 B 查看记录 WHOIS 缺陷的报告列表。

c. 成果

2013 年 6 月 24 日，EWG 发布了初步报告、常见问题解答和在线问卷调查，启动了就其初步建议在 ICANN 机构群体内广泛征询意见的流程。在初步报告中，EWG 认为应当舍弃授予每位用户相同的匿名公共访问权来访问（往往不准确的）gTLD 注册数据的当前 WHOIS 模式。同时，EWG 建议实行范式转换，确保 gTLD 注册数据的收集、验证和披露仅用于容许目的，并规定某些数据元素仅限通过身份验证的请求者访问且只能用于合理目的。

在提出这一建议前，EWG 充分考虑了机构群体过去发布的旨在阐述 WHOIS 缺陷的报告以及许多使用当前 WHOIS 系统的不同利益主体。对于每一个已确定的用户群体，EWG 分析了他们使用注册数据和个人数据元素的目的。基于这一分析结果，EWG 提出了用以指导建立下一代注册目录服务 (RDS) 的原则和特性。为了说明如何践行这些原则，EWG 还考虑了多个备选方案，并提出了一种收集和披露准确域名注册数据元素以用于容许目的的模式。

2013 年 11 月 11 日，在认真考虑了 ICANN 机构群体提交的所有意见和反馈后，EWG 发布了一份状态更新报告，其中强调了 EWG 对许多关键问题的看法。应机构群体的要求，此状态更新报告还提供了关于在初步报告之后开展的分析的大量细节。

随后，EWG 对就这两份报告收到的反馈进行了详细分析，以机构群体提出的大量多样化意见为基础，继续开展其在开放式领域内的工作，测试和完善相关建议。考虑到手头任务的复杂性以及下一代 RDS 必须建立在充分了解其可能带来的益处和影响的基础上，EWG 对五个方面进行了研究：当前的 ccTLD 和商业数据验证实践、当前的隐私/代理服务提供商实践、对有能力认证 RDS 用户的组织的探究以及 RDS 风险/益处和成本的分析。此次研究的结果已于 2014 年 3 月发布，并被 EWG 用于进一步完善建议。

在现阶段，EWG 仔细考虑了以下方面：过去在 WHOIS 领域所做的工作、gTLD 注册数据的现有用户和未来可能用户及他们的目的、当前 WHOIS 系统内众多不同利益主体的意见、与拟议 RDS 改进措施相关的当前实践以及对 RDS 风险、益处和成本的分析。所有这些资料都是 EWG 在提出关于下一代系统的建议[5]时的参考对象，同时也将是政策制定流程的重点参考对象，相关内容已在提交给 ICANN 理事会的本最终报告中详细阐述。

[5] 在本报告的 EWG 原则中，下列词语采用 RFC 2119 中给出的释义：

- MUST（必须）：与“REQUIRED”（必需）或“SHALL”（必须）一样，表示该定义对象对本报告而言是绝对要求。
- MUST NOT（不可以）：与短语“SHALL NOT”（不得）一样，表示该定义对象对本报告而言是绝对禁止。
- SHOULD（应该）：与形容词“RECOMMENDED”（建议的）一样，表示在特定情况下可能存在忽略某一事项的正当理由，但在选择不同做法前必须了解和仔细权衡忽略所带来的全部影响。
- SHOULD NOT（不应该）：与短语“NOT RECOMMENDED”（不建议）一样，表示在特定情况下可能存在某特定行为变为可接受甚至有用的正当理由，但在实施任何带有此标签的行为前必须了解其带来的全部影响，仔细权衡具体情况。

III. 用户和目的

a. 方法

在定义下一代注册目录服务时，EWG 尽量从零开始，而不是在被广泛认为存在不足的当前 WHOIS 系统上进行改进。按照理事会的指示，EWG 从研究收集和存储 gTLD 注册数据以及向广大用户提供这类数据的现有和潜在目的开始着手分析。

为了达到这一目标，EWG 成员挑选了大量涉及当前 WHOIS 系统的实际使用案例，并对每个案例进行了分析，明确了以下几点：(i) 想要访问数据的用户，(ii) 他们访问这些数据的理由，(iii) 他们需要访问哪些数据元素，以及 (iv) 这些数据将用于什么目的。此外，EWG 还利用这些案例来明确所有涉及收集、存储和提供注册数据的利益主体，以便了解现有的工作流程和方式以及利用下一代 RDS 可能更好地满足用户及其需求的潜在工作流程和方式。

这些使用案例虽然并非详尽无遗，但它们代表了当前 WHOIS 系统的许多使用情况，说明了各种各样的用户、需求和工作流程。请参见 附录 C 查看 EWG 考虑的使用案例目录。

为了整理出 RDS 必须涵盖的利益主体和所需目的，明确系统必须加以阻止的一系列潜在滥用行为（参见本报告下一节），EWG 考虑了这些使用案例的总体情况和从中获得的经验。此外，EWG 还参考了以前的 WHOIS 相关活动的参考资料、机构群体意见以及使用案例，旨在研究下面图 1 中所示的各个领域的具体需求。

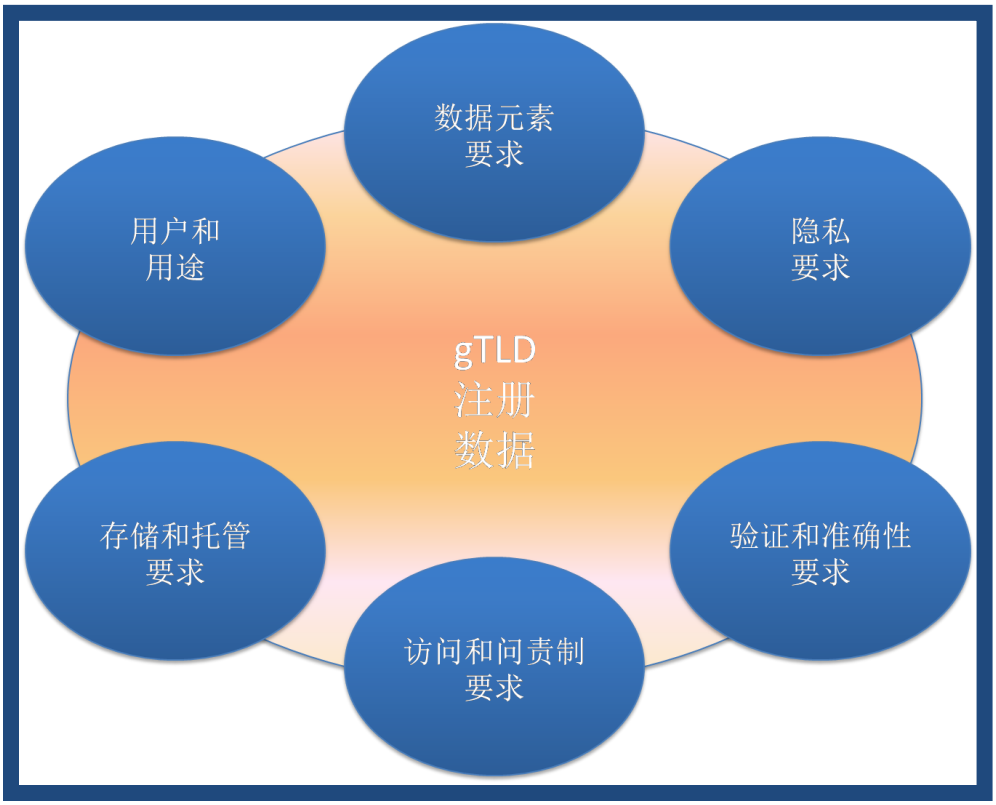


图 1：需求分析

随后，EWG 继续分析了这些目的和用户需求，明确了各个目的的最低数据元素要求、提供这类数据所带来的风险和对隐私法及政策的影响，以及本报告中探讨的其他问题。

b. RDS 用户和目的

下方的图 2 大致总结了现有 WHOIS 系统的用户，其中既有出于建设性目的的，也有出于恶意目的的。依据 EWG 的使命，EWG 对所有这些用户都进行了核查，确定了现有工作流程和未来可能的工作流程，以及流程涉及的利益主体和数据。

图 2：用户

在本报告中，术语“请求者”泛指这些用户中任何希望从系统中获取 gTLD 注册数据的人。正如本报告将详细讨论的那样，EWG 建议舍弃授予每位用户相同的匿名公共访问权来访问（往往不准确的）gTLD 注册数据的当前 WHOIS 模式。同时，EWG 建议实行范式转换，确保 gTLD 注册数据的收集、验证和披露仅用于容许目的，并规定某些数据元素仅限通过身份验证的请求者访问且只能用于合理目的。

EWG 分析了这些具有代表性的使用案例，制作出以下表格，该表总结了想要访问 gTLD 注册数据的用户类型、需要访问的理由以及这些数据的整体用途。关于各类用户、目的和相应数据需求的详细信息，请参见第 III(c) 节“需要满足或禁止的目的”和附录 D。

用户	目的	使用案例示例	访问注册数据的理由
所有注册人 （如，自然人、法人、经认证的隐私/代理服务提供商）	域名控制	域名注册帐户创建	使任何类型的注册人都能通过在注册服务商下创建新帐户来注册域名
		域名数据修改监测	检测域名注册数据（无论是当前的还是过去的[使用 WhoWas]）是否遭到意外、不知情或未经授权的修改
		域名投资组合管理	便于更新所有域名注册数据（如，指定联系人、地址等）以维护域名投资组合
		域名迁移启动	使注册人能够发起向另一注册服务商的域名迁移
		域名删除	能删除过期域名

用户	目的	使用案例示例	访问注册数据的理由
		域名 DNS 更新	使注册人能够发起对某一域名的 DNS 变更
		域名续用	使域名注册人能够续用已注册的域名
		域名联系信息验证	便于注册人对域名注册数据（如，指定联系人、地址等）进行初始和持续验证
受保护的注册人（如，需要联系的经认证隐私/代理服务客户）	个人数据保护	联系隐私/代理服务提供商	使任何希望最大限度减少对个人姓名及地址进行公共访问的注册人都能与经认证的隐私或代理注册服务提供商取得联系
		联系安全凭证批准方	使受到威胁的个人或群体能够利用可信第三方授予的安全凭证与提供注册服务的经认证安全凭证批准方取得联系
互联网技术人员（如，DNS 管理员、邮件管理员、网络管理员、ISP）	解决技术问题	联系域名技术人员	便于联系能帮助解决域名技术或运营问题（如，DNS 解析失败、电子邮件发送问题、网站功能问题）的技术人员（个人、职能角色或实体）
证书颁发机构	域名认证	签发域名认证	帮助证书颁发机构 (CA) 确定域名注册人是否与 SSL/TLS 证书绑定
互联网个人用户（如，消费者）	个人互联网使用	联系现实世界	帮助消费者获得域名注册人的非互联网联系信息（如，办公地址）
		消费者保护	为消费者提供一种轻量化机制，便于消费者在没有 LE/OpSec 干预的情况下联系域名注册人指定的业务联系人（如，网上零售商客户服务），从而快速解决问题
互联网企业用户（如，品牌持有人、经纪人、代理人）	企业域名的购买或销售	通过经纪人销售域名	允许对域名的购买进行调查
		域名商标通关	在创立新品牌时能对域名注册人进行鉴定以支持商标通关（风险分析）
		域名收购	使收购者能与注册人联系以便收购之前已注册的域名
		域名购买查询	能确定域名可用性以及当前注册人和管理联系人（如有）
		域名注册历史记录	提供域名注册历史记录，以便通过 WhoWas 确定过去的注册人和注册日期
		指定注册人注册的域名	能在合并/剥离资产验证时确定由指定实体注册的所有域名（反向查询）
互联网研究员	学术/公众利益 DNS 研究	域名注册历史记录	使研究员能在学术/符合公众利益的 DNS 研究时对域名注册的历史进行研究 (WhoWas)

用户	目的	使用案例示例	访问注册数据的理由
		指定联系人注册的域名	在符合公众利益的学术研究中，能够根据给定姓名、地址、域名服务器、注册日期等确定相应的所有域名（反向查询）
		调查域名注册人或指定联系人	使研究员能够调查域名注册人或其指定的联系人
知识产权所有者（如，品牌持有人、商标所有者、知识产权所有人）	法律诉讼	域名用户联系信息	针对因商标/品牌侵权或知识产权盗窃而正在接受调查的域名，能够与使用该域名的当事方联系
		打击对注册人数据的欺诈性使用行为	便于通过对经过身份验证的数据进行反向查询，识别对属于另一注册人的域名合法数据（如，地址）的欺诈性使用并作出响应
		域名注册历史记录	能在研究知识产权侵权时对域名注册的历史进行研究 (WhoWas)
		指定注册人注册的域名	能在研究知识产权侵权时找出注册在某一给定姓名或地址下的所有域名（反向查询）
非 LEA 调查员（如，税务机构人员、UDRP 提供商、ICANN 合规工作人员）	监管和合同的执行	网上税务调查	便于国家、州、省或地方税务机构找出网上销售的域名的联系人
		UDRP 程序	让 UDRP 提供商负责确认正确的域名应诉人、执行合规性检查、确定法律流程要求以及防止域名规避
		RDS 生态系统的合同合规性	让 ICANN 审核和处理针对签约方不遵守规定的投诉（如，数据不准确或不可用、UDRP 裁决的实施、迁移投诉、数据托管与保存）
LEA/OpSec 调查员（如，执法机构、事件响应小组）	犯罪调查和减少 DNS 滥用	调查遭到滥用的域名	使 LEA/OpSec 人员能对所谓的恶意注册域名展开有效调查和收集证据，包括检查历史数据
		调查离线犯罪活动	通过提供详细的注册数据和/或搜索注册在疑犯名下的域名（反向查询），使 LEA/OpSec 人员能对离线犯罪活动展开有效调查和收集证据
		域名声誉服务	使域名声誉服务提供商能对域名白/黑名单进行分析
		调查网络犯罪活动	帮助受害者或其法律顾问找出涉嫌参与非法活动的域名注册人，使 LE/OpSec 能进一步展开调查
		被攻击域名的滥用问题联系人	帮助 LEA/OpSec 人员联系域名注册人或其指定的滥用问题联系人以协助修复受攻击域名

用户	目的	使用案例示例	访问注册数据的理由
普通大众 （如，博主、媒体人、政治活动家）	DNS 透明度	访问公共注册数据	满足广大互联网用户的共同期望，帮助他们明确在具体使用案例中不会反映出来的、域名“背后”的组织
恶意者 （如，参与发送垃圾邮件、发起 DDoS 攻击、网络钓鱼、身份盗窃、域名劫持的人）	互联网恶意活动	域名劫持	获取域名注册数据，非法访问注册人帐户并劫持该注册人的域名
		恶意注册域名	利用现有/受攻击域名的注册帐户来注册新域名以便从事犯罪、欺诈或滥用活动
		挖掘注册数据用于发送垃圾邮件/进行网络诈骗	获取域名注册人数据供垃圾邮件发送者、诈骗者以及其他犯罪分子（恶意者）恶意使用

表 1：RDS 用户和目的

c. 需要满足或禁止的目的

为了专注于开发使用案例和缩小容许目的的范围，EWG 曾试图给上面列举的目的排定优先级。然而，若只满足现在访问当前 WHOIS 系统的一些用户的需求而忽略其他人的需求，这似乎无道理可言，因为其他人的访问目的也同样没有恶意。鉴于此，EWG 建议，除了应该加以积极阻止的已知恶意互联网活动以外，对于所有已确定的容许目的，RDS 都应*以某种方式*给予满足。EWG 建议的容许目的如下图所示。

图 3：容许目的

应该指出的是，对于每一种目的，现在和将来都有无数使用案例。尽管 EWG 没有尝试研究所有可能的使用案例，但努力研究了具有代表性的案例样本，希望能明确用户类型以及他们访问 gTLD 注册数据的目的。不过，由于随着时间的流逝，不断有新用户和容许目的涌现，因此 RDS 在设计时必须被赋予容纳这些新用户和容许目的的职能。

在分析了众多使用案例（如附录 C 所列）之后，EWG 发现，许多用户虽然出于不同的访问目的，但其需要访问的数据元素却很类似。在这些需求中，有些很容易理解，比如：

- 用以确定某一域名是否已经注册
- 用以确定域名的当前状态
- 用以联系与域名相关的某人

不过，也有一些需求虽然是许多用户共同的需求，但当前 WHOIS 系统却并未以相同的方式加以满足。例如：

- 用以确定某一已知实体注册的所有域名（通常称为“反向 WHOIS”）
- 用以确定域名注册的历史信息（通常称为 WhoWas）

EWG 在起草本报告中的 RDS 建议时详细考虑了这些共同需求。不过，由于后面不断会有其他共同需求涌现，因此，EWG 在设计时应牢记任何下一代系统都必须赋予可扩展性这一点。下表列出了 EWG 目前已确定的容许目的及相应的注册数据、联系信息和查询需求。

目的	定义
域名控制	包括创建、管理和监控注册人自己的域名 (DN)，如创建域名、更新域名信息、迁移域名、续用域名、删除域名、维护域名投资组合和检测是否有人对注册人自己的联系信息进行欺诈性使用。这就意味着，出于这一访问目的的所有注册人都必须是经过身份验证的 RDS 用户，可以在 RDS 内访问与其域名相关的所有公共信息和网关信息，包括在 RDS 内发布的该域名的指定联系人数据。
个人数据保护	包括确定某一域名的经认证隐私/代理服务提供商以报告滥用行为、请求披露或出于其他原因联系提供商。为了达到这类目的，用户需要可靠、方便地联系隐私/代理服务提供商 — 例如，通过隐私/代理服务提供商 PBC 的滥用问题相关 URL，访问说明提供商披露流程或允许用户提交披露申请表的页面。
解决技术问题	包括努力解决与域名使用相关的技术问题，如电子邮件发送问题、DNS 解析失败和网站功能问题等。为了达到这类目的，用户需要能够与负责处理这些问题的技术人员取得联系。（注：指定多个分别负责解决不同问题的联系点可能可行，例如负责解决电子邮件问题的邮件管理员。）

目的	定义
域名认证	包括证书颁发机构(CA) 向某一域名对应的主体签发 X.509 证书。为了达到这一目的，用户需要确认该域名确实注册在该证书主体名下；而确认这一事项需要访问关于相应注册人的所有公共数据和网关数据。
个人互联网使用	包括明确使用域名的组织以培养消费者信任，或联系该组织以提交客户投诉或提交对该组织的投诉。为了达到这类目的，用户需要获得该组织的名称（最好先通过身份验证）及合法（邮政）地址，此外，通过联系人 URL 访问描述组织及其客户服务联系人或允许用户提交客户服务查询的页面可能对用户有所帮助。
企业域名的购买或销售	包括域名购买查询、收购另一注册人的域名以及开展尽职调查研究。为了达到这类目的，用户需要访问注册人的组织和电子邮件地址，某些情况下可能还需要访问其他网关数据，例如，根据注册人或联系人的姓名进行反向查询以找出与该注册人或联系人关联的其他域名。
学术/公众利益 DNS 研究	包括针对 RDS 内所发布域名开展符合公众利益的学术研究，如关于注册人和指定联系人的信息、域名的历史信息和状态以及注册在某一已知注册人名下的域名（反向查询）。为了达到这类目的，用户需要能够访问 RDS 内的所有公共数据，某些情况下可能还需要访问网关数据并通过匿名、汇总形式使用这类数据。
法律诉讼	包括调查其他域名对注册人姓名或地址的可能欺诈性使用、调查可能的商标侵权、在采取法律诉讼前联系注册人/被许可人的法律代表并在问题无法得到圆满解决后采取法律诉讼。为了达到这类目的，用户需要能够在没有经认证隐私/代理服务提供商转达的情况下，与注册人/被许可人的法律代表直接取得联系。
监管和合同的执行	包括税务机构利用在线服务对企业进行调查、UDRP 调查、合同合规性调查以及注册数据托管审核。为了达到这类目的，经认证的用户需要访问某些网关的注册人联系数据和域名数据元素，如邮政地址和电话号码等，具体视用户陈述的目的而定。例如，WIPO 可能需要访问 UDRP 裁决。
犯罪调查和减少 DNS 滥用	包括向能够调查和解决滥用行为的人报告这类行为，或在离线犯罪调查期间联系与某一域名相关的实体。为了达到这类目的，经认证的用户（如，执法人员、第一响应者）需要迅速、可靠地与负责相关域名的滥用问题联系人取得联系，例如，通过访问某一 URL 了解滥用行为报告流程或提交事件报告表。
DNS 透明度	包括查询注册人公布的注册数据以满足各种旨在使公众知情的用例需求。为了达到这类目的，用户需要能够轻松访问 RDS 提供的公共数据（仅限公共数据）。必须通知注册人他们的域名注册公共数据可能会被用于这一“全局性”目的，且此目的必须仅限于使用公共数据（即，用户不得为达到这一目的而访问网关数据）。

表 2：目的定义

下表进一步总结了实现这些目的所需的注册数据范围，包括涉及的域名、所需数据的种类（注册人数据、联系人数据、域名数据）以及所需的其他查询。

目的	查询范围	所需联系人	所需注册人数据	DN 数据	所需其他查询
域名控制	自己的 DN	所有	公共+网关	是	反向（自己的数据） WhoWas（自己的 DN）
个人数据保护	PP DN*	PP	公共	是	无
解决技术问题	任意 DN	技术	公共	是	无
域名认证	任意 DN	无	公共+网关	是	无
个人互联网使用	LP DN*	业务	公共	否	无
企业域名的购买或销售	任意 DN	管理	公共+经批准的网关	是	反向（经批准的数据） WhoWas（任意 DN）
学术/公众利益 DNS 研究	任意 DN	所有	公共+经批准的网关	是	反向（经批准的数据） WhoWas（任意 DN）
法律诉讼	任意 DN	法务	公共+经批准的网关	是	反向（经批准的数据） WhoWas（任意 DN）
监管和合同的执行	任意 DN	法务	公共+网关	是	反向（任意数据） WhoWas（任意 DN）
犯罪调查和减少 DNS 滥用	任意 DN	滥用	公共+网关	是	反向（任意数据） WhoWas（任意 DN）
DNS 透明度	任意 DN		公共	是	无

表 3：各个目的所需的注册数据范围

按照“服务条款”的规定，表 3 中的“经批准的网关数据”可定义为经认证 RDS 用户在满足下列既定政策时可进行申请的数据：

- 哪些用户有资格申请网关数据
- 申请网关数据的正当理由
- 网关数据的使用限制
- 为确保合理使用而需要进行的监督

ICANN 应参考 RDS 用户群体的意见，对需要“经批准的网关数据”的目的展开进一步分析，确定如何合理地定义、实施和执行这类政策，实现问责制和隐私保护之间的平衡。为了说明具体可以如何操作，我们列举了以下几个例子：

- **学术/公众利益 DNS 研究**：例如，如果一位来自经认可大学、从事某一特定 DNS 研究领域的研究员需要访问网关数据，他必须先列出所需的网关数据元素和这些数据的使用方式，同意仅以汇总/匿名的形式发布研究结果，同时接受独立审查委员会 (IRB) 的监督。在获得可以执行“公众利益 DNS 研究”的批准后，经认证 RDS 用户便有权访问某些特定的网关注册人数据元素或利用反向查询功能查询这些数据元素。
- **域名购买/销售**调查：例如某一从事商业交易的企业用户需要尽职调查卖家持有的域名资产。这种情况下，可要求该企业用户在认证机构（参见第 IV(c) 节“RDS 用户认证”中的定义）的监控和监督下，证明他们是涉及域名购买的买家以及 RDS 数据对尽职调查卖家“X”而言必不可少的这两点，同时规定调查结果只能用于这一特定的交易目的。在获得可以使用 DNS 执行这类尽职调查的批准后，经认证 RDS 用户便有权通过反向查询功能、利用经批准网关数据查询卖家“X”持有的域名，详细说明请参见附录 E。
- **法律诉讼**调查：例如某一执业律师调查商标侵权。这种情况下，可要求该用户在认证机构（参见第 IV(c) 节“RDS 用户认证”）的监控和监督下，证明其正在调查一桩可能的法律诉讼以及 RDS 数据对调查相应标的物“Y”而言必不可少这两点，同时规定所有返回数据只能用于这一特定目的。在获得可以使用 DNS 执行这类商标侵权调查的批准后，经认证 RDS 用户便有权通过反向查询功能、利用经批准网关数据查询与标的物“Y”相关的域名，详细说明请参见附录 E。

关于这些目的如何与 RDS 数据相关、经批准网关数据扮演什么角色以及可以采取哪些保障措施来确保用户负责和防止滥用行为，请参见附录 E“网关访问和无验证访问说明”。

通过以上对 RDS 用户和容许目的的研究，EWG 制定出了可实现基于目的的注册数据访问的基本原则，如下表所示：

编号	容许目的原则
1.	ICANN 必须集中发布一份说明注册数据使用目的和容许目的的通俗易懂的政策，使注册人明白收集注册数据的原因以及处理和使用这类数据的方式。
2.	必须明确定义 RDS 的容许/不容许目的。

3.	RDS 必须为已明确定义的容许目的的提供支持，这些目的包括： • 为达到某一特定目的而需要找出域名的注册人及其指定联系人； • 为达到某一特定目的而需要与指定联系人取得联系； • 使用注册管理机构发布的关于域名的数据；以及 • 为达到某一特定目的而需要查询部分注册数据。
4.	RDS 在设计时必须被赋予容纳随时间不断涌现的新用户和容许目的的职能。 • 必须制定明确的申请流程 • 必须按照既定标准对申请进行审核 • 通过审核的申请必须经过多利益主体复核委员会的评估和批准，该委员会由政策制定流程确定 • 经批准的申请必须纳入 RDS 隐私政策中，并按照政策规定定期实施（如，每季度、每年） 注：请参见第 VI 节“数据元素”了解新数据元素的添加流程。
5.	对于所有已确定的容许目的，RDS 都应*以某种方式*给予满足，但已知的恶意互联网活动除外，这类活动必须加以积极阻止。EWG 建议的容许目的如表 1“RDS 用户和目的”和图 3“容许目的”所示。
6.	gTLD 注册数据的收集、验证和披露应仅用于容许目的，而且某些数据元素应仅限通过身份验证的请求者访问且只能用于合理目的。
7.	必须给予所有注册人访问 RDS 内与其自己域名相关的所有公共和网关信息的能力，包括指定联系人的数据。

d. RDS 中涉及的利益主体

下表总结了负责收集、存储、披露和使用 gTLD 注册数据的各种具有代表性的利益主体，并给出了与其对应的目的。其中，某些利益主体主要负责提供数据（如，注册人），而其他利益主体则负责收集/存储数据（如，验证方、注册服务商、注册管理机构）或披露数据（如，RDS 提供商、经认证的隐私/代理服务提供商）。不过，大多数利益主体都是发起数据请求的当事方（如，品牌持有者及其代理人等）或因为披露的数据而被识别、联系或受此类数据影响的当事方（如，域名滥用联系人）。该表旨在让人们了解 RDS 很可能影响到的利益主体的广度。而且，在涉及注册数据的任何交易中，还可能存在此处未列举出来的其他利益主体。

利益主体	目的
域名滥用联系人	犯罪调查和减少滥用
收购公司	企业域名的购买或销售
收购公司的代理人/律师	企业域名的购买或销售
地址验证服务	域名控制
注册人的代理人	域名控制
品牌持有人	监管/合同的执行
品牌管理服务提供商	域名控制
品牌所有者	企业域名的购买或销售
证书颁发机构	域名认证
投诉人	监管/合同的执行
网购的消费者	个人互联网使用
访问网站的互联网用户	个人互联网使用
域名经纪人	企业域名的购买或销售
域名买家	企业域名的购买或销售
诈骗受害者	法律诉讼
诈骗受害者的代理人	法律诉讼
政府机构人员	监管/合同的执行
ICANN 合规工作人员	监管/合同的执行
独立审查委员会 (IRB)	学术/公众利益 DNS 研究
互联网服务提供商	解决技术问题 犯罪调查和减少滥用
调查员	个人互联网使用
执法人员	犯罪调查和减少滥用 法律诉讼
登记的隐私/代理服务提供商联系人	个人数据保护 域名控制 学术/公众利益 DNS 研究
登记的技术联系人	解决技术问题 域名控制 学术/公众利益 DNS 研究
登记的管理联系人	监管/合同的执行 域名购买/销售 域名控制 学术/公众利益 DNS 研究
登记的法务联系人	法律诉讼 监管/合同的执行 学术/公众利益 DNS 研究
登记的业务联系人	个人互联网使用 域名控制 学术/公众利益 DNS 研究
登记的滥用联系人	犯罪调查和减少滥用 域名控制 学术/公众利益 DNS 研究
在线服务提供商	解决技术问题
Op/Sec 服务提供商	犯罪调查和减少滥用
研究赞助机构	符合公众利益的 DNS 域名研究
受到调查的个人/实体	监管/合同的执行
隐私/代理服务客户	企业域名的购买或销售

	域名控制 解决技术问题 监管/合同的执行 个人数据保护
隐私/代理服务提供商	犯罪调查和减少滥用 企业域名的购买或销售 域名控制 符合公众利益的 DNS 域名研究 解决技术问题 法律诉讼 个人数据保护 监管/合同的执行 解决技术问题
RDS 提供商	所有目的
注册人	所有目的
注册人的法务联系人	法律诉讼 监管/合同的执行
注册服务商	企业域名的购买或销售 域名控制 符合公众利益的 DNS 域名研究 个人互联网使用 法律诉讼 个人数据保护 监管/合同的执行 解决技术问题 犯罪调查和减少滥用
注册管理机构	所有目的
问题报告人	解决技术问题
研究员	学术/公众利益 DNS 研究
分销商	域名控制 犯罪调查和减少滥用
问题解决者	解决技术问题
法律/民事诉讼的对象 **寻求联系的第三方**	个人互联网使用 法律诉讼 个人数据保护
安全凭证批准方	个人数据保护
安全凭证接收者	个人数据保护
UDRP 专家小组成员	监管/合同的执行
UDRP 提供商	监管/合同的执行
验证方	所有目的
滥用受害者	犯罪调查和减少滥用
Web 托管服务提供商	解决技术问题

表 4：代表性利益主体一览表

e. 基于目的的联系人原则

公有区域内的互联网域名及其使用会给全世界第三方带来诸多潜在的外部影响。从滥用行为到技术问题再到侵权和大大小小的域名问题，位于世界某个地方的第三方总有各种理由需要与某一特定域名相关的人或组织进行联系。

而另一方面，域名注册人可能希望并且也有权利（取决于当地的管辖权）保护自己的隐私。他们可能不希望将自己的详细联系信息公之于众。而且，注册人往往并不是解决第三方所提问题（例如，与域名 DNS 配置或解决商标争议相关的问题）的最佳人选或实体。因此，仅仅披露注册人信息可能无法满足第三方寻求解决域名相关问题的需求。

此外，潜在问题的多样性决定了所需解决方案在内容和及时性方面也各不相同，从理论上而言，不同问题往往需要与特定域名相关的不同人和/或组织加以解决。不过，任何域名都必须至少公布一个或多个信息准确、能联系到的联系人负责响应外部查询，以及为受域名存在或运营影响的外部参与者提供容许目的的参考。

对特定联系人类型而言，响应的及时性可以作为政策制定的一个预期目标。不过，这一目标必须考虑到响应需求对负责满足这些需求的实体造成的负担。如因系统博弈、不当请求或故意给联系人造成重负而引起响应不及时，则这些联系人不应受到任何处罚。ICANN 可以制定相应的流程，使出于某些目的（如，处理滥用问题、响应 UDRP 申请）请求访问、但联系人未作出任何响应的请求者可以报告这一沟通失败事件。未回应此类流程可能会导致联系人停用和/或删除，同时可能会对确认流程中的域名造成影响。不过，具体的响应及时性政策目标不在本报告的讨论范围之内。

编号	基于目的的联系人原则
8.	每个已注册的域名必须至少提供一名负责披露所有强制性 PBC 的所有强制性数据元素的“基于目的的联系人”(PBC)。为确保满足每个既定容许目的的需求，该 PBC 就语法而言必须准确，就操作性而言必须可联系到。
9.	在域名注册期间，注册人的联系人 ID[6] 必须作为所有目的的默认 PBC ID 使用。必须告知注册人所有容许目的，并为其提供针对每一项目的公布其他 PBC ID 的机会，包括替换针对任意目的或所有目的的注册人联系人 ID。

[6] 为方便检索和更新，联系人 ID 采用与联系人数据块相关联的标识符，这一概念在第 IV(a) 节“数据元素”中引入，并在第 V(d) 节“联系人 ID 的运作机制”中加以定义。

编号	基于目的的联系人原则
10.	基于目的的联系人不一定非得是注册人，而且按照其他政策的规定，对注册人信息的访问可能是高度控制的。请注意，PBC 并不一定是某一具体的人，也可能是负责响应各种目的的指定联系点。
11.	在针对各个适用目的提供有效的 PBC ID 之前，不得对域名进行激活（即放入全球 DNS 中）。如果某一 PBC 无法继续响应其指定目的，则必须启动相应的流程，使注册人能够在允许的 PBC ID 合理更新时限内，执行更新通知以及指定新的有效的联系人。此阶段内，正如上面的原则 #9 所述，注册人的联系人 ID 必须作为所有目的的默认 PBC ID 使用。如果注册人未在该时限内提供有效的 PBC ID，则可能导致域名在确认流程中遭到停用和/或删除。（参见第 V 节“验证”要求。）
12.	可视需要为各个容许目的提供 PBC ID，针对各类 PBC 需收集和发布的数据元素规定不同的访问要求，以满足相应容许目的的需求。
13.	必须制定适当的流程和政策，使由注册人指定的联系人能自行选择是否将自己的联系人 ID 作为域名的 PBC ID 公布，为个人和实体提供接受或拒绝在特定域名注册中担任特定职责的权利。
14.	用于提供“基于目的的联系人”的系统必须具有一定的灵活性，允许在 RDS 内创建和发布新的目的和联系人类型。（请参见第 III(c) 节，了解更多关于添加新目的的详细信息。）

f. 基于目的的联系人角色和职责

EWG 分析了各种具有代表性的使用案例，明确了希望访问 gTLD 注册数据的用户类型以及当前可使用这些数据的容许目的，大致情况请参见图 4 和表 1。为了使用户能对注册数据进行基于目的的访问，EWG 将所有容许目的与 PBC 进行了关联。例如：

- 可指定“法务”联系人负责处理与域名相关的商标争议或其他法定要求。为了让用户能与之取得联系，该 PBC 仅需提供一个能接收法律通知的实际地址、一个用于接收询问的有效电子邮件地址以及一个用于接收查询的工作电话或传真号码。
- 可指定“滥用”联系人负责处理与通过域名滥用带来不正常流量或其他具有高度时效性的恶意互联网活动相关的调查。为了让用户能与之取得联系，该 PBC 必须提供一个能接收和响应有效投诉的电子邮件地址以及一个用于接收询问的有效电话号码。当然，PBC 也可以提供方便实时互动的社交媒体和即时通讯地址、接收查询的实际地址或传真号码以及方便报告滥用行为的公开 URL。

PBC 也可以指定自己的经认证隐私/代理服务提供商、管理、技术和业务联系人。完整的 PBC 类型及相应职责列表请参见表 5；另请参见第 IV 节“数据收集原则 #20”了解各类 PBC 负责的数据元素需求。

如下图所示，如注册人未提供某一给定域名的具体 PBC，则 EWG 建议使用注册人自己的 ID。例如，如果注册人没有为给定域名指定具体的法务联系人，则注册人应了解到：当用户为达到相关容许目的的时，他们可能需要联系注册人；此时注册人仍然有机会指定 PBC 负责接收关于该域名的此类请求。

如果注册人选择不指定 PBC，则用户将通过与注册人的联系人 ID 相关联的、此目的所需的数据将这类请求发送给注册人。如果注册人不希望公开这些数据元素，其可以使用经认证的隐私/代理服务来注册域名。更多关于数据元素原则和 PBC 的讨论，请参见第 IV 节。

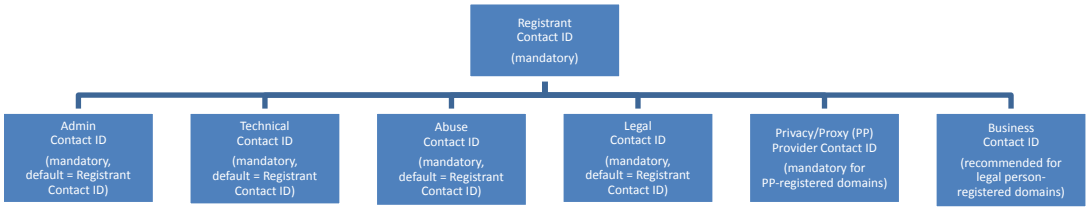


图 4：RDS 联系人类型

所有目的/联系人必须由政策制定者通过规定的目的添加、更改或删除流程编纂成文。

本 PBC 方法不仅能满足基本的联系需求还能满足更为广泛的联系需求，既能简化注册人的工作也能为注册人提供更多粒度。为了说明这一概念，下面给出了三个虚构但相当典型的例子：

1. 注册人可以明确指定自己的联系人 ID 为域名的唯一联系点。这种情况下，所有容许目的的 RDS 查询将根据不同目的的不同需求，返回与注册人联系人 ID 关联的经授权公共或网关数据元素。

域名记录示例：

```
注 册 人 联 系 人   ID  =  <reg>
技 术 联 系 人   ID  =  <reg>
管 理 联 系 人   ID  =  <reg>
滥 用 问 题 联 系 人   ID  =  <reg>
法 务 联 系 人   ID  =  <reg>
```

2. 使用经认证**隐私**服务（见第 VII 节中的定义）的注册人可以为自己的域名指定多个唯一联系人 ID，包括隐私/代理服务提供商的联系人 ID（即，隐私服务提供商）、技术联系人 ID（如，托管服务商或 ISP）和提供商提供的管理、滥用及法务联系人 ID。这种情况下，指定技术联系人将负责解决与域名相关的所有技术问题，经认证隐私/代理服务提供商将负责与域名相关的所有隐私服务（包括将管理、滥用和法务联系人信息转发给注册人）。

域名记录示例：

```
注册人联系人 ID = <reg>
PP 联系人 ID = <pp>
技术联系人 ID = <isp>
管理联系人 ID = <reg@pp>
滥用问题联系人 ID = <reg@pp>
法务联系人 ID = <reg@pp>
```

3. 选择将自己身份界定为法人的注册人可以为某一给定域名提供许多唯一的联系人 ID，包括与该域名相关的法务、滥用和业务 PBC ID。这种情况下，针对各类目的请求的 RDS 查询将返回与相应 PBC ID 关联的数据元素，使请求者能直接与负责指定事务的个人或实体取得联系。将来，大型组织会更多地采用这种粒度来提高可联系性和减少错误传达及重定向，因此这种情况可能会越来越普遍。

域名记录示例：

```
注册人联系人 ID = <reg>
技术联系人 ID = <isp>
管理联系人 ID = <admin@reg>
滥用问题联系人 ID = <abuse@reg>
法务联系人 ID = <legal@reg>
业务联系人 ID = <cs@reg>
```

下图较为直观地对这些例子进行了说明：

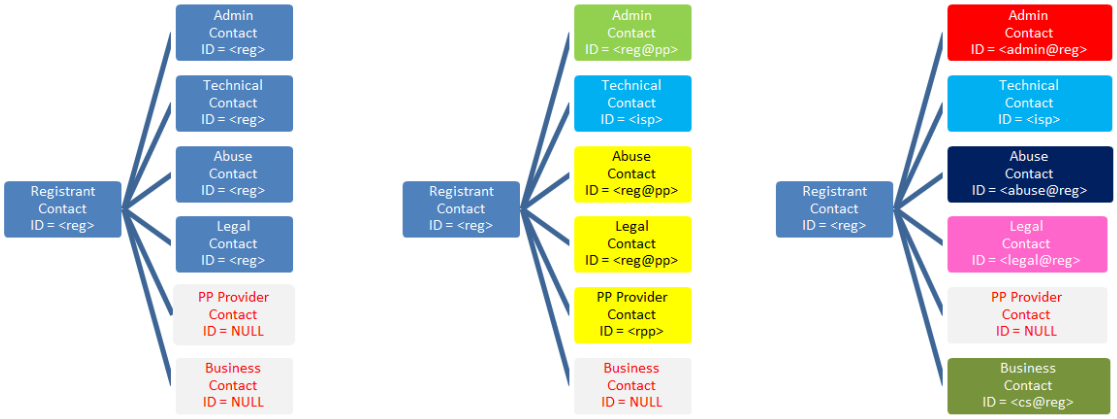


图 5：使用基于目的的联系人的域名注册示例

请参阅第 IV 节查看建议 PBC 列表，参阅附录 D 查看与各个容许目的相关的数据元素及相应 PBC 完整列表。

PBC 职责包括接收关于该域名的请求、评估请求以及确认请求和/或通知注册人/被许可人，所有操作都必须根据注册人与 PBC 之间的合同协议执行。

各类 PBC 的可能职责大致如下：

PBC 类型	可能职责
管理	处理与域名收购和销售相关的请求，如购买咨询和域名迁移。
法务	处理税务机构、UDRP 调查员、合同合规性调查员和法律代表提出的关于域名的请求。
技术	处理针对域名提出的与网站中断、DNS 问题、电子邮件发送问题等相关的请求。
滥用	处理关于域名的 DNS 滥用报告，包括网络钓鱼、垃圾邮件和其他有害的互联网活动。
隐私/代理	处理传达/披露请求，以注册人/被许可人的名义提出关于域名滥用的投诉，对犯罪活动进行 LEA 调查。
业务	处理消费者的信息访问请求，如业务信息以及用来联系公司以获取更多信息或解决消费者投诉的联系信息。

表 5：各类基于目的的联系人的可能职责

供将来考虑：可以为每一类 PBC 指定多个 PBC，这样用户便可直接与负责相关事务的具体个人联系。例如，对于一个大型的互联网组织，可以将众多技术问题分为几个较小的范畴，分别由邮件管理员、DNS 操作员、网站管理员等负责，并在作为公共数据发布的字段中对这种专项联系人的职务进行标记，以明确注册人指定 PBC 负责的具体目的。虽然就现阶段而言，要实现这一复杂的结构不太合理，但不排除将其纳入将来的考虑范围之内。

g. RDS 联系人使用授权

如上文所述，域名注册指定的 PBC 数量必须至少符合最低要求。所有这些联系人必须了解并同意履行注册人就每个被注册域名为其指定的职责。有关这一概念的原则如下所列。

编号	基于目的的联系人使用授权原则
15.	每个 PBC 必须能够以灵活、实时或接近实时的方式授予批准，以免延误域名注册或域名更新。
16.	政策和流程必须防止有人未经授权而对 PBC 加以利用。
17.	PBC 或注册人必须具备在日后撤销批准的能力。（请参见第 V 节“验证”了解详细信息）

编号	基于目的的联系人使用授权原则
18.	注册人必须具备在不经外部/第三方批准的情况下轻松指定自己为域名 PBC 的能力。

例如，注册人可以提供能够立即被负责该联系人 ID 的验证方自动验证的 PBC 联系人 ID 和一次性使用令牌。或者，也可以通过在流程中部署电子邮件或手机短信验证系统来获取联系人授权。

IV. 加强问责制

EWG 建议的 RDS 采取一切归零、从头开始的方式，舍弃当前“一刀切”的 WHOIS 系统，支持公众以目的为导向访问经验证的数据，以此加强隐私保护和问责制，提高准确性。

EWG 相信，这种网关的访问模式定能加强对所有涉及披露和使用 gTLD 域名注册数据的相关方的责任追究。首先，RDS 会记录所有访问 gTLD 注册数据的行为，包括未经身份验证的公共数据元素访问和旨在阻止批量获取的限制访问。其次，较为敏感的数据元素仅限提出申请并通过 RDS 查询验证和获颁相应凭证的请求者进行网关访问。最后，RDS 会对公共数据访问和网关数据访问进行审查，以最大限度减少滥用，并对不当使用行为给予处罚和采取其他补救措施。对于不同目的可应用不同的条款和条件。一旦违反了这些条款和条件，请求者将受到相应的处罚。

目前，已有许多 ICANN 机构群体成员对舍弃完全匿名的公共 WHOIS 而支持 EWG 建议的网关访问模式表示担忧。其中，部分成员建议向完全匿名的请求者公开所有注册数据，而其他成员则建议只公开很小一部分数据或不公开任何数据。一些人对认证出于容许目的请求访问数据的用户这一概念表示支持，但要求提供更多关于以下方面的细节信息：可用数据元素、认证流程以及如何制定和逐步完善与容许目的相关的政策。鉴于目前尚未找到可以满足这些不同意见的简单答案，本节将从这几个方面详细讨论 EWG 的建议。

a. 数据元素原则

EWG 建议按照以下原则对数据元素进行分类。

编号	数据元素原则
19.	RDS 必须具备以目的为导向披露数据元素的职能。（请参见第 III 节查看有关容许目的及相应的基于目的的联系人 (PBC) 的列表。）
20.	并非所有收集的数据都可向公众披露；是否披露必须取决于请求者及其使用目的。

编号	数据元素原则
21.	必须允许对经确认的最小数据集的公共访问，包括明确公布以方便沟通的 PBC 数据。
22.	对于在风险和影响评估后确定为较敏感的数据元素，必须通过网关访问加以保护，只有在以下情况下才允许披露： • 确认属于容许目的 • 已知请求者/使用目的 • 通过审核/合规性检查确保网关访问没有遭到滥用
23.	只能披露允许用于宣称目的的数据元素（即，以响应的形式返回或通过反向查询和 WhoWas 查询进行搜索）。
24.	所有收集的数据元素都必须至少具有一个容许目的。
25.	每个数据元素必须具有一组容许目的。 • 本报告给出了一组初始的可接受用途、容许目的和数据元素需求（请参见第 III 节和附录 D）。 • 每个容许目的必须具有已明确定义的数据元素访问和使用政策。 • 如第 III 节所述，必须制定持续的审核流程来考虑新提出的目的和定期更新容许目的以添加新批准的目的，并将这些目的与现有的数据元素关联起来。 • 必须制定相应的政策定义流程，以考虑新提出的数据元素，并在必要时更新已定义的数据元素，将其与现有容许目的关联起来。
26.	待收集、存储和披露的最小数据元素列表必须根据已知使用案例（见本文档相关内容）和风险评估（在实施 RDS 前完成）来确定。
27.	所有注册管理机构和验证方必须对他们为 RDS 收集/提供的完整数据元素集进行存储。（另请参见第 VII 节“可能的 RDS 模式”。）

步骤 1：数据收集

在为达到容许目的而选择性地披露数据前，必须先收集数据。EWG 建议在注册时按照以下原则收集数据：

编号	数据收集原则
28.	为了满足第 VI 节提出的首要法律原则，注册服务商和验证方应在数据收集时，为域名注册人和基于目的的联系人提供选择机会，让他们决定是否同意用户在遵守相应管辖区内的数据保护法的前提下，将其数据用于预先披露的容许目的。在制定政策时，ICANN 必须在更大的背景下遵循这些首要法律原则，以满足本数据收集原则。[7]
29.	为了满足基本的域名控制需求，在注册域名时，注册管理机构和注册服务商必须收集、同时注册人必须提供以下数据元素： a. 域名 b. DNS 服务器 c. 注册人姓名 d. 注册人类型 表明与注册人姓名或名称对应的实体的类型，便于应用适当的注册数据要求，如下： **未声明** — 如果没有选中以下任何选项，则按默认情况规定注册数据要求，且该注册人必须按对待自然人的方式进行对待。 **隐私/代理服务提供商** — 通过经认证隐私/代理服务提供商注册域名时必须选择此项。选择的同时必须提供经认证隐私/代理服务提供商的联系人 ID，以便将传达/披露请求报告给 PP PBC。 **法人** — 在将域名注册在非自然人、非代理服务提供商的实体名下时可选择此项。选择的同时必须提供指定业务 PBC 的联系人 ID，以便处理消费者的查询和投诉。（请参见表后的注释。） **自然人** — 在将域名注册在自然人名下时可选择此项。选择的同时既无需提供隐私/代理 PBC 也无需提供业务 PBC，且注册人的姓名和地址须视为个人信息，受到数据主体所在管辖区内适用数据保护法的保护。 e. 注册人联系人 ID 在验证期间分配给每位注册人联系人的唯一 ID [姓名+地址]（请参阅第 V 节，了解关于联系人 ID 的详细定义、如何通过验证方创建联系人

[7] 除一位 EWG 成员提出异议以外，其他成员均对这一原则表示一致支持。

编号	数据收集原则
	ID 以及如何将其用于域名注册） f. 注册人邮政地址 包括以下数据元素：街道、城市、州/省、邮编、国家/地区（如适用） g. 注册人电子邮件地址 h. 注册人电话 包括以下数据元素：电话号码、分机号码（如适用）
30.	a. 为了在加强注册人隐私保护的同时提高其可联系性，注册服务商必须收集、同时注册人必须提供每个已注册域名的“基于目的的联系人”(PBC)。 b. 注册人可以选择指定隐私/代理服务提供商提供的 PBC 或经授权的第三方 PBC 来响应特定容许目的（请参见第 III 节）。 c. 为了满足各个容许目的的沟通需求，经验证方创建并随后与域名相关联的 PBC 必须符合下列最低强制性数据元素要求： 技术联系人：电子邮件地址 管理联系人：所属组织、电子邮件地址 法务联系人：所属组织、电子邮件地址、电话号码、邮政地址 滥用问题联系人：电子邮件地址、电话号码 业务联系人[8]：所属组织、邮政地址 隐私/代理服务提供商联系人[9]：所属组织、电子邮件地址、联系人 URL、滥用 URL d. 默认情况下，如果注册人未指定各强制性容许目的的 PBC，则这些 PBC 将使用注册人自己的联系人 ID。（注：注册人可通过使用经认证的隐私/代理服务或通过指定 PBC 来避免这种情况发生。）一旦注册人自己的联系人 ID 作为 PBC ID 使用，针对注册人数据的收集和披露要求便会相应地增加，以满足上述 PBC 强制性数据元素需求。
31.	为了避免收集的数据超出需求，对于注册人提供的、未在第 29 或 30 条原则中列出但却用于一个以上容许目的的数据，注册人可自行决定收集与否。如果注册人选择收集，则验证方、注册管理机构和注册服务商必须为这类数据的收集和存储提供条件。

[8] 仅当注册人类型 = 法人时此联系人才为强制性数据元素

[9] 仅当注册人类型 = 隐私/代理服务提供商时此联系人才为强制性数据元素

编号	数据收集原则
32.	为了最大限度提高互联网的稳定性，注册管理机构和注册服务商必须向 RDS 提供以下强制性数据元素： a. 注册状态 b. 客户端状态（由注册服务商设定） c. 服务器状态（由注册管理机构设定） d. 注册服务商 e. 注册服务商所在辖区 f. 注册管理机构所在辖区 g. 注册协议语言 h. 创建日期 i. 注册服务商到期日期 j. 更新日期 k. 注册服务商 URL l. 注册服务商 IANA 号码 m. 注册服务商滥用问题联系人电话号码 n. 注册服务商滥用问题联系人电子邮件地址 o. Internic 投诉站点 URL
33.	对于 TLD 专用的数据元素，TLD 注册管理机构必须制定和发布相应的数据收集政策（与这些首要原则保持一致），并负责验证这些专用数据元素。
34.	在不与 RDS 共享的情况下，验证方、注册管理机构和注册服务商可以收集、存储或披露其他数据元素供内部使用。[10]

注：经过多番讨论之后，EWG 最终未提出将**域名用途**添加为数据元素这一建议。相反，EWG 提出了诸多旨在实现相关目标的原则建议，同时，它还建议以**法人**身份从事商业活动的注册人公布明确的**业务 PBC**。这可能会使许多商业互联网用户在意识到注册人最终会选择这一类数据之后，纷纷通过更为一致地发布数据元素来提高消费者信心，而且，要在全球范围内严格区分域名用途 = 商业还是非商业几乎是不可能的。

[10] 例如，在域名注册期间供客户使用的 IP 地址、请求生成域名 EPP 迁移密钥的链接以及与客户账户相关的支付数据。数据的内部使用并未经过 RDS 规范化，而是由注册管理机构和注册服务商私下定义的。

步骤 2：数据披露

数据收集完成后，便可针对容许目的对其进行选择性披露。EWG 建议在收到查询请求时按照以下原则披露数据：

编号	数据披露原则
35.	为了最大限度保护注册人的隐私，默认情况下注册人提供的数据必须处于封闭状态，当公众存在迫切的访问需求且这种需求大于所产生风险时除外。 • 注册人可以在知情同意后，选择将任何封闭的注册人数据公开。
36.	为了最大限度提高互联网的稳定性，所有由注册管理机构或注册服务商提供的注册数据必须保持公开，除非这一做法会导致不可接受的风险。 • 除了必须公开以满足下述基本域名控制需求的情况以外，注册人可以选择将任何公开的注册管理机构/注册服务商数据封闭。
37.	为了最大限度提高可联系性，默认情况下所有 PBC 都必须面向公众公开。 • 联系人持有者[11]可以选择将任何 PBC 数据元素封闭，除非必须公开以满足指定目的（更多详细信息请参见表 5）。
38.	为了满足基本的域名控制需求，最小公共数据集必须包含注册人提供的以下数据，这些数据均属于必须收集且披露风险较低的类型： a. 域名 b. DNS 服务器 c. 注册人类型 d. 注册人联系人 ID（详细定义请参见第 V 节） e. 注册人电子邮件地址 f. 技术联系人 ID g. 管理联系人 ID h. 法务联系人 ID i. 滥用问题联系人 ID j. 隐私/代理服务提供商的联系人 ID （仅当注册人类型 = 隐私/代理服务提供商时才为强制性数据元素） k. 业务联系人 ID

[11] 根据第 III(g) 节“RDS 联系人使用授权”的阐述，指定 PBC 必须在给定的域名注册范围内授权使用联系人 ID。同时，这也意味着联系人持有者同意请求者出于该目的公共/封闭使用其数据。不过，若预验证 PBC 不包含可以实现给定目的的强制性/公共数据元素，则无法将该 PBC 指定为这一目的的 PBC。

编号	数据披露原则
	（仅当注册人类型 = 法人时才为强制性数据元素）
39.	为了实现简单与可联系性的平衡，必须让注册人知道：若注册人不提供强制性 PBC，则他/她的联系人 ID 将被用作该 PBC，且注册人数据元素将作为域名的技术联系人、管理联系人、法务联系人和滥用联系人予以公布。要避免这类数据披露，注册人可指定一个或多个第三方 PBC，或使用经认证的隐私/代理服务（这种情况下，那些地址数据将由服务提供商提供）。
40.	对于 TLD 专用的数据元素，TLD 注册管理机构必须制定和发布相应的数据披露政策（与这些首要原则保持一致），并负责识别任何 TLD 专用数据元素的容许目的。

产生的数据元素分类

以上述原则为基础，下表详细列出了 EWG 建议的各个 RDS 数据元素分类，其中的字母含义如下：

- M 和 O 分别用于定义数据元素的收集是强制的还是可选的。这意味着：

  [1] 对从注册人处收集的数据而言，
  M 表示数据的收集是强制的，即必须由注册服务商/验证方提出请求，然后由注册人提供；而
  O 表示数据的收集是可选的，即必须由注册服务商/验证方提出请求，但是否提供则由注册人根据是否适用这一原则自行决定。

  [2] 对从基于目的的联系人持有者处收集的数据而言，
  M 表示数据的收集是强制的，即必须由注册服务商/验证方提出请求，然后由联系人持有者提供；而
  O 表示数据的收集可选的，即必须由注册服务商/验证方提出请求，但是否提供则由联系人持有者根据是否适用这一原则自行决定。以及

R（建议的）表示数据的收集必须由注册服务商/验证方提出请求，但是否提供所请求数据则由联系人持有者根据是否适用这一原则自行决定，以反映“最佳”和“良好”实践建议[12]

[3] 对注册管理机构和注册服务商向 RDS 提供的数据而言，

M 表示数据的收集是强制的，即注册管理机构/注册服务商必须提供数据，而 O 表示数据的收集是可选的，即既可以提供数据也可以不提供数据，具体视情况而定。

- P 和 G 用于定义数据元素是公开数据元素[无论是否通过身份验证，所有人均可访问]还是网关数据元素[仅限通过身份验证的用户访问且只能用于容许目的]，Y/N 定义注册人能否更改默认的披露设定。这意味着：

[4] 对从注册人处收集的数据而言，

P / N 表示所有收集的数据必须公开，不能隐藏；

P / Y 表示所有收集的数据在默认情况下是公开的，但注册人可以选择将其隐藏；

G / Y 表示所有收集的数据在默认情况下是网关数据，但注册人可以在知情同意的情况下，选择将其公开。

[5] 对注册管理机构和注册服务商向 RDS 提供的数据而言，

P / N 表示所有提供的数据必须公开，不能隐藏；而

G / N 表示所有提供的数据必须是网关数据，目前暂无属于这一类别的数据元素。

[6] 对从基于目的的联系人持有者处收集的数据而言，

P / N 表示所有收集的数据必须公开，不能隐藏；

P / Y 表示所有收集的数据在默认情况下是公开的，但联系人持有者可以选择将其隐藏

请注意，已知用户是否可以访问网关数据元素取决于具体的容许目的。一旦注册人选择将默认的网关元素公开，任何人便可对该元素进行访问。而一旦注册人选择将默认公开的元素变成网关元素，则该元素仅限出于容许目的的用户访问。

[12] EWG 关于发布各种 PBC 数据元素的最佳实践建议是基于 EWG 成员的运营经验而提出的。强制性元素是指要达到相应目的需要满足的最低运营要求。不过，实际上，若对于某一给定目的已存在相应的沟通方式（例如，用于报告问题的网页表单，替代为用电子邮件来联系技术人员），则该替代方式极其有用，往往是处理问题的首选沟通方式。当然，不同 PBC 采用的替代方式也有所相同，例如，邮政地址对联系法务或业务联系人非常有用，但对联系滥用或技术联系人以快速解决问题却基本无用。因此，EWG 对每一类 PBC 中的数据元素分别提出了具体的建议。

注册管理机构/注册服务商提供的数据	收集 M 或 O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [3]“收集定义” 和 [5]“披露定义”
注册状态	**M**	**P**	**N**	
DNSSEC 授权	O	**P**	**N**	
客户端状态 （注册服务商）	**M**	**P**	**N**	包含注册服务商级别的 所有域名适用值： DeleteProhibited（禁止删除）、 RenewProhibited（禁止续用）、 TransferProhibited（禁止迁移）
服务器状态 （注册管理机构）	**M**	**P**	**N**	未包含在 RAA 中， 与客户端状态类似， 但为注册管理机构级别
注册服务商	**M**	**P**	**N**	
分销商	O	**P**	**N**	
注册服务商所在辖区	**M**	**P**	**N**	未包含在 RAA 中
注册管理机构所在辖区	**M**	**P**	**N**	未包含在 RAA 中
注册协议语言	**M**	**P**	**N**	未包含在 RAA 中
创建日期	**M**	**P**	**N**	
原始注册日期	O	**P**	**N**	未包含在 RAA 中
注册服务商到期日期	**M**	**P**	**N**	
更新日期	**M**	**P**	**N**	
注册服务商 URL	**M**	**P**	**N**	
注册服务商 IANA 号码	**M**	**P**	**N**	
注册服务商滥用问题联系人电子邮件地址	**M**	**P**	**N**	
注册服务商滥用问题联系人电话号码	**M**	**P**	**N**	
Internic 投诉站点 URL	**M**	**P**	**N**	

从注册人处收集的 注册人数据	收集 M 或 O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [1]“收集定义” 和 [4]“披露定义”
域名	**M**	**P**	**N**	
DNS 服务器	**M**	**P**	**N**	
注册人姓名	**M**	G	Y	
注册人类型	**M**	**P**	**N**	
注册人联系人 ID	**M**	**P**	**N**	替换注册管理机构注册人 ID， 由验证方在 RDS 中分配
注册人联系人验证状态	**M**	**P**	**N**	新增，由验证方提供
注册人联系人上次验证 时间戳	**M**	**P**	**N**	新增，由验证方提供
注册人组织	O	**P**	Y	当注册人类型 = 法人或代理服务 提供商时收集
注册人公司标识符 （如，商业名称、 D-U-N-S）	O	**P**	Y	由邓白氏公司等机构向企业签发 的实际标识符 当注册人类型 = 法人 时收集 未不包含在 RAA 中
注册人街道地址	**M**	G	Y	
注册人所在城市	**M**	G	Y	
注册人所在州/省	O	G	Y	按照 2013 RAA 的规定， 所有“州/省”数据元素都应在 适用时加以收集
注册人邮编	O	G	Y	按照 2013 RAA 的规定， 所有“邮编”数据元素都应在 适用时加以收集
注册人所在国家/地区	**M**	G	Y	
注册人电话 + 分机	**M**	G	Y	分机号码仅在适用时收集
注册人备用电话 + 分机	O	G	Y	新选项，未包含在 RAA 中
注册人电子邮件地址	**M**	**P**	**N**	
注册人备用电子邮件	O	**P**	Y	新选项，未包含在 RAA 中
注册人传真 + 分机	O	G	Y	按照 2013 RAA 的规定，所有 “传真号”和“传真分机号”数 据元素都应在适用时加以收集
注册人 SMS	O	G	Y	新选项，未包含在 RAA 中
注册人 IM	O	G	Y	新选项，未包含在 RAA 中
注册人社交媒体	O	G	Y	新选项，未包含在 RAA 中
注册人备用社交媒体	O	G	Y	新选项，未包含在 RAA 中
注册人联系人 URL	O	G	Y	新选项，未包含在 RAA 中
注册人滥用 URL	O	G	Y	新选项，未包含在 RAA 中

基于目的的联系人 管理联系人	收集 M/R/O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [2]“收集定义” 和 [6]“披露定义”
目的：域名购买/销售、域名控制、DNS 研究				
管理联系人 ID	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	未包含在 RAA 中
PBC 验证状态	**M**	**P**	**N**	新增，由验证方提供
PBC 上次验证时间戳	**M**	**P**	**N**	新增，由验证方提供
PBC 名称	**M**	**P**	**N**	
PBC 所在组织	**M**	**P**	**N**	
PBC 街道地址	R	**P**	Y	
PBC 所在城市	R	**P**	Y	
PBC 所在州/省	O	**P**	Y	
PBC 邮编	O	**P**	Y	
PBC 所在国家/地区	**M**	**P**	**N**	
PBC 电话 + 分机	O	**P**	Y	
PBC 备用电话 + 分机	O	**P**	Y	未包含在 RAA 中
PBC 电子邮件地址	**M**	**P**	**N**	
PBC 备用电子邮件地址	O	**P**	Y	未包含在 RAA 中
PBC 传真 + 分机	O	**P**	Y	
PBC 短信号码	O	**P**	Y	未包含在 RAA 中
PBC 即时通讯地址	O	**P**	Y	未包含在 RAA 中
PBC 社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 备用社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 联系人 URL	O	**P**	Y	未包含在 RAA 中
PBC 滥用 URL	O	**P**	Y	未包含在 RAA 中

基于目的的联系人 法务联系人	收集 M/R/O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [2]“收集定义” 和 [6]“披露定义”
目的：法律诉讼、监管/合同、域名控制、DNS 研究				
法务联系人 ID	**M**	**P**	**N**	未包含在 RAA 中
PBC ID	**M**	**P**	**N**	未包含在 RAA 中
PBC 验证状态	**M**	**P**	**N**	新增，由验证方提供
PBC 上次验证时间戳	**M**	**P**	**N**	新增，由验证方提供
PBC 名称	**M**	**P**	**N**	
PBC 所在组织	**M**	**P**	**N**	
PBC 街道地址	**M**	**P**	**N**	
PBC 所在城市	**M**	**P**	**N**	
PBC 所在州/省	O	**P**	Y	
PBC 邮编	O	**P**	Y	
PBC 所在国家/地区	**M**	**P**	**N**	
PBC 电话 + 分机	**M**	**P**	**N**	
PBC 备用电话 + 分机	O	**P**	Y	未包含在 RAA 中
PBC 电子邮件地址	**M**	**P**	**N**	
PBC 备用电子邮件地址	O	**P**	Y	未包含在 RAA 中
PBC 传真 + 分机	**R**	**P**	**Y**	
PBC 短信号码	O	**P**	Y	未包含在 RAA 中
PBC 即时通讯地址	O	**P**	Y	未包含在 RAA 中
PBC 社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 备用社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 联系人 URL	O	**P**	Y	未包含在 RAA 中
PBC 滥用 URL	O	**P**	Y	未包含在 RAA 中

基于目的的联系人 技术联系人	收集 M/R/O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [2]“收集定义” 和 [6]“披露定义”
目的：解决技术问题、域名控制、DNS 研究				
技术联系人 ID	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	未包含在 RAA 中
PBC 验证状态	**M**	**P**	**N**	新增，由验证方提供
PBC 上次验证时间戳	**M**	**P**	**N**	新增，由验证方提供
PBC 名称	R	**P**	Y	
PBC 所在组织	R	**P**	Y	
PBC 街道地址	R	**P**	Y	
PBC 所在城市	R	**P**	Y	
PBC 所在州/省	O	**P**	Y	
PBC 邮编	O	**P**	Y	
PBC 所在国家/地区	**M**	**P**	**N**	
PBC 电话 + 分机	**R**	**P**	Y	
PBC 备用电话 + 分机	**R**	**P**	Y	未包含在 RAA 中
PBC 电子邮件地址	**M**	**P**	**N**	
PBC 备用电子邮件地址	**R**	**P**	Y	未包含在 RAA 中
PBC 传真 + 分机	O	**P**	Y	
PBC 短信号码	**R**	**P**	Y	未包含在 RAA 中
PBC 即时通讯地址	**R**	**P**	Y	未包含在 RAA 中
PBC 社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 备用社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 联系人 URL	**R**	**P**	Y	未包含在 RAA 中
PBC 滥用 URL	O	**P**	Y	未包含在 RAA 中

基于目的的联系人 滥用问题联系人	收集 M/R/O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [2]“收集定义” 和 [6]“披露定义”
目的：减少滥用、域名控制、DNS 研究				
滥用问题联系人 ID	**M**	**P**	**N**	未包含在 RAA 中
PBC ID	**M**	**P**	**N**	未包含在 RAA 中
PBC 验证状态	**M**	**P**	**N**	新增，由验证方提供
PBC 上次验证时间戳	**M**	**P**	**N**	新增，由验证方提供
PBC 名称	R	**P**	Y	
PBC 所在组织	R	**P**	Y	
PBC 街道地址	R	**P**	Y	
PBC 所在城市	R	**P**	Y	
PBC 所在州/省	O	**P**	Y	
PBC 邮编	O	**P**	Y	
PBC 所在国家/地区	**M**	**P**	**N**	
PBC 电话 + 分机	**M**	**P**	**N**	
PBC 备用电话 + 分机	O	**P**	Y	未包含在 RAA 中
PBC 电子邮件地址	**M**	**P**	**N**	
PBC 备用电子邮件地址	O	**P**	Y	未包含在 RAA 中
PBC 传真 + 分机	O	**P**	Y	
PBC 短信号码	O	**P**	Y	未包含在 RAA 中
PBC 即时通讯地址	**R**	**P**	Y	未包含在 RAA 中
PBC 社交媒体地址	**R**	**P**	Y	未包含在 RAA 中
PBC 备用社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 联系人 URL	**R**	**P**	Y	未包含在 RAA 中
PBC 滥用 URL	**R**	**P**	**Y**	未包含在 RAA 中

基于目的的联系人 隐私/代理 (PP) 提供商联系人	收集 M/R/O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [2]“收集定义” 和 [6]“披露定义”
目的：个人数据保护、域名控制、DNS 研究				
PP 联系人 ID	**M**	**P**	**N**	未包含在 RAA 中
PBC ID	**M**	**P**	**N**	未包含在 RAA 中
PBC 验证状态	**M**	**P**	**N**	新增，由验证方提供
PBC 上次验证时间戳	**M**	**P**	**N**	新增，由验证方提供
PBC 名称	**M**	**P**	**N**	
PBC 所在组织	**M**	**P**	**N**	
PBC 街道地址	**M**	**P**	**N**	
PBC 所在城市	**M**	**P**	**N**	
PBC 所在州/省	O	**P**	Y	
PBC 邮编	O	**P**	Y	
PBC 所在国家/地区	**M**	**P**	**N**	
PBC 电话 + 分机	**M**	**P**	**N**	
PBC 备用电话 + 分机	O	**P**	Y	未包含在 RAA 中
PBC 电子邮件地址	**M**	**P**	**N**	
PBC 备用电子邮件地址	O	**P**	Y	未包含在 RAA 中
PBC 传真 + 分机	O	**P**	Y	
PBC 短信号码	O	**P**	Y	未包含在 RAA 中
PBC 即时通讯地址	O	**P**	Y	未包含在 RAA 中
PBC 社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 备用社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 联系人 URL	**M**	**P**	**N**	未包含在 RAA 中
PBC 滥用 URL	**M**	**P**	**N**	未包含在 RAA 中

基于目的的联系人 业务联系人	收集 M/R/O	默认 披露 P 或 G	能否更改 披露 设定？	备注 参见 [2]“收集定义” 和 [6]“披露定义”
目的：个人互联网使用、域名控制、DNS 研究				
业务联系人 ID	**M**	**P**	**N**	未包含在 RAA 中
PBC ID	**M**	**P**	**N**	未包含在 RAA 中
PBC 验证状态	**M**	**P**	**N**	新增，由验证方提供
PBC 上次验证时间戳	**M**	**P**	**N**	新增，由验证方提供
PBC 名称	**M**	**P**	**N**	
PBC 所在组织	**M**	**P**	**N**	
PBC 街道地址	**M**	**P**	**N**	
PBC 所在城市	**M**	**P**	**N**	
PBC 所在州/省	O	**P**	Y	
PBC 邮编	O	**P**	Y	
PBC 所在国家/地区	**M**	**P**	**N**	
PBC 电话 + 分机	R	**P**	Y	
PBC 备用电话 + 分机	O	**P**	Y	未包含在 RAA 中
PBC 电子邮件地址	R	**P**	Y	
PBC 备用电子邮件地址	O	**P**	Y	未包含在 RAA 中
PBC 传真 + 分机	O	**P**	Y	
PBC 短信号码	O	**P**	Y	未包含在 RAA 中
PBC 即时通讯地址	O	**P**	Y	未包含在 RAA 中
PBC 社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 备用社交媒体地址	O	**P**	Y	未包含在 RAA 中
PBC 联系人 URL	**R**	**P**	**Y**	未包含在 RAA 中
PBC 滥用 URL	O	**P**	Y	未包含在 RAA 中

另外，EWG 再次建议开展一次大范围的风险/影响分析，确认这些基于原则的分类是否真的能实现出于特定目的的合理数据收集和披露。

按 2013 RAA 进行调整与新增数据元素

目前，为了便于过渡和理解，所有由 EWG 建议的数据元素名称都已尽可能按照 2013 RAA 中定义的名称进行调整（如，DNSSEC 授权、RDS 失效日期）。不过，2013 RAA 中使用的数据元素名称并不足以反映 EWG 建议的基于目的的联系人（请参见第 III 节）。在调整时，EWG 进行了以下映射：

当 RDS 管理联系人 ID 指 PBC 时，
RDS PBC 名称 = RAA 管理联系人姓名
RDS PBC 所在组织 = RAA 管理联系人所在组织
其他 RAA 管理联系人数据元素以此类推

当 RDS 技术联系人 ID 指 PBC 时，
RDS PBC 名称 = RAA 技术联系人姓名
RDS PBC 所在组织 = RAA 技术联系人所在组织
其他 RAA 技术联系人数据元素以此类推

注：EWG 建议在 RDS 门户上提供各类 PBC 的定义，方便 RDS 用户访问（例如，使用悬停弹出定义），以此明确表明 PBC 可处理众多出于容许目的的查询请求，同时 EWG 还建议必须指定一个涵盖这些目的的联系点。注册人可以选择自己接收查询请求（将注册人 ID 指定为 PBC）、让经认证的隐私/代理服务提供商接收这些查询（让 PP 提供相应的数据元素 — 通常是转发地址或提供商的地址）或指定某一具体的实体接收这些查询（如，服务提供商、托管服务商、法定代理人、客户服务中心等）。

除 2013 RAA 中定义的数据元素以外，建议新增元素如下：

注册服务商和注册管理机构管辖区：在注册服务商和注册管理机构与 ICANN 所签协议中定义的两者的运营法律辖区。

注册协议语言：注册服务商与注册人之间所签合同使用的语言。

原始注册日期：域名首次注册的日期。[13]

客户端状态、服务器状态：由 2013 RAA 中的客户端状态值扩展而来，这些数据元素包含当前应用于该域名的注册服务商（客户端）和注册管理机构（服务器）状态值：DeleteProhibited（禁止删除）、RenewProhibited（禁止续用）、TransferProhibited（禁止迁移）。

注册人公司标识符：英国商业编号、D-U-N-S 号码或其他由公共业务目录分配给注册人的唯一实体公司标识符。这类标识符允许在 RDS 以外搜索某一公司。

[13] 该日期与创建日期不同，后者是指域名最近一次注册的日期；有可能域名在注册后被删除多次。而原始注册日期是指域名首次注册的日期，在这之前该域名从未注册过。

注册人联系人 ID：分配给经过预验证的联系人数据块的唯一句柄，该数据块与域名的注册人相关联。请参阅第 V 节，了解关于联系人 ID 的详细定义以及如何创建和使用联系人 ID。此 ID 使在 RDS 内重复使用和维护联系人数据变得可能。请注意，当注册人类型 = 隐私/代理服务提供商时，注册人联系人 ID 将反映分配给该经认证隐私/代理服务提供商的唯一标识符。

注册人/PBC 联系人的验证状态、注册人/PBC 联系人上次验证时间戳：注册人/PBC 联系人接受的最高验证级别以及最近一次验证的日期，详细定义请参见第 V 节。

注册人/PBC 短信号码、即时通讯地址、社交媒体地址：可选择通过短信、即时通讯或其他替代社交媒体通信载体联系注册人或 PBC 的新联系方式。

注册人/PBC 备用电子邮件地址、备用电话号码、备用社交媒体地址：当使用第一联系地址无法联系到注册人或 PBC 时，可选择使用这些新增的备用地址。这些新数据元素旨在满足一些常见需求，例如在域名本身宕机时解决技术问题，以及通过手机或社交媒体更迅速地取得联系。

注册人/PBC 联系人 URL、滥用 URL：新数据元素，可选择通过它们访问提供有滥用行为报告说明、政策或表单的相关网页，提高沟通效率。

PBC 联系人 ID：分配给经过预验证的联系人数据块的唯一句柄，该数据块在“联系人角色”指定的角色中与域名的 PBC 相关联。注册人联系人 ID 与 PBC 联系人 ID 既可以指同一联系人，也可以指不同的联系人。

注：在开始实施 RDS 前，必须先考虑这些新数据元素带来的过渡和合规性挑战。

b. 无需身份验证的数据访问原则和网关数据访问原则

EWG 提出了一种新的注册数据访问方法，建议舍弃任何人可完全匿名访问任何数据的当前模式，采用同时结合公共访问某些数据与封闭访问其他数据的新模式。与这一建议对应的原则如下所列。

编号	数据访问原则
41.	必须向未经身份验证的 RDS 用户提供最小数据元素集，同时确保至少符合最严格的隐私政策。
42.	根据所述的容许目的，为经过身份验证的用户提供不同级别的数据访问。
43.	RDS 用户访问凭证的认证流程必须具有可审核性，详细定义请参见第 IV(c) 节“RDS 用户认证”。

编号	数据访问原则
44.	所有访问必须遵循无歧视原则（即，访问流程必须为所有出于同一目的的请求者创建一个公平竞争的环境）。
45.	为了防止滥用和加强问责制： • 所有数据元素访问必须建立在所述目的的基础上； • 网关数据元素必须仅限于声称用于容许目的且通过身份验证的请求者访问；以及 • 请求者必须具备申请和接收凭证的能力，以便在将来需经过身份验证的数据访问查询中使用。
46.	必须对封闭访问的请求者实施某种类型的认证： • 对经认证的请求者而言，他们必须在每次提出数据查询请求时陈述一遍自己的目的。 • 对于不同目的可应用不同的条款和条件。 • 一旦违反了这些条款和条件，经认证的请求者必须受到相应处罚。
47.	为了提高 gTLD 注册数据的保护标准，所有 RDS 查询/响应必须采用普遍使用的消息加密和验证措施，确保数据在传输过程中的保密性和完整性。
48.	为了满足经验证 RDS 用户达到容许目的的需求，RDS 必须提供反向查询服务，使用户能通过某一特定值搜索相关的公共和网关数据元素，同时返回引用该值的所有域名列表。
49.	为了满足经验证 RDS 用户达到容许目的的需求，RDS 必须提供 WhoWas 服务，向用户返回指定域名的公共和网关数据元素历史快照，但这仅限于 RDS 内拥有的历史数据。
50.	RDS 必须为利用 RDS 数据元素的创新服务提供支持，如下： • 必须确保第三方能够利用公共数据元素提供现有和未来的创新服务（包括反向查询和 WhoWas），同时第三方必须遵守 RDS 数据使用的条款和条件。 • 若第三方提供的创新服务涉及网关数据元素，则这些第三方必须先经过认证，且必须遵守 RDS 数据使用的条款和条件。

编号	数据访问原则
51.	网关数据元素的披露必须采用已定义的 RDS 访问方式（包括上文讨论的方式）。用户不得通过未受控制的访问批量导出全部 gTLD 的整个 RDS 数据集（或单个 gTLD 的整个注册管理机构数据集）。
52.	可通过交互显示和其他 RDS 访问方式披露数据。 • 为了能始终如一地轻松找到数据和访问数据，必须建立一个访问中心（如，门户网站）。 • 必须确保所有请求者都能通过无需身份验证的查询方式对公共数据进行安全访问（至少可通过安全网站访问）。 • 对于经过身份验证的请求者和使用目的，必须确保请求者能通过安全网络和其他访问方式及格式（如，RDAP xml 响应、短信、电子邮件）对网关数据进行安全访问。 • 必须确保请求者能在有需要时实时从 RDS 中获得权威数据。 • RDS 必须具备自动对各种使用案例和容许目的进行大规模查找的功能。
53.	为实现真正的全球化，RDS 必须能以多种语言、文字和字符集显示注册数据（包括国际化域名 (IDN)）。
54.	RDS 应支持 GNSO 将来为 gTLD 制定的所有翻译政策。
55.	RDS 应能够以当地语言收集和显示注册数据元素。

公共数据访问说明

如下图所示，无论是否通过身份验证，任何人均可以向 RDS 请求访问公共数据元素。请参阅附录 E，了解更多关于响应未经身份验证公共数据查询而返回的数据元素的详细说明。

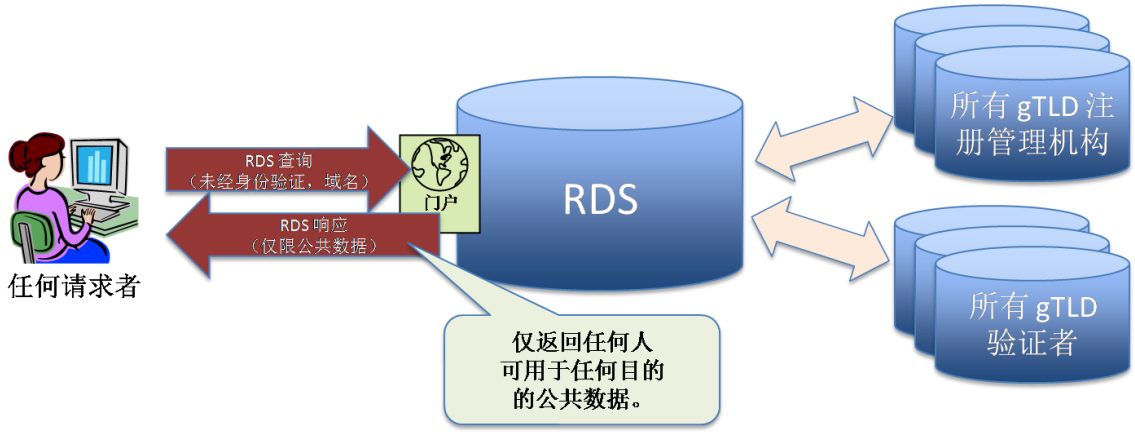


图 6：通过 RDS 对公共注册数据进行未经验证的访问

附录 I 中也提供了相关的流程图和使用案例示例，旨在阐明相关数据元素的访问步骤。

网关数据访问说明

如下图所示，网关数据元素也可以通过 RDS 请求访问。不过，要访问这类数据，请求者必须先通过认证。随后，请求者可以出于已陈述的目的提交经过身份验证的数据元素查询请求。请参阅附录 E，了解更多关于响应经身份验证网关数据查询而返回的数据元素的详细说明。

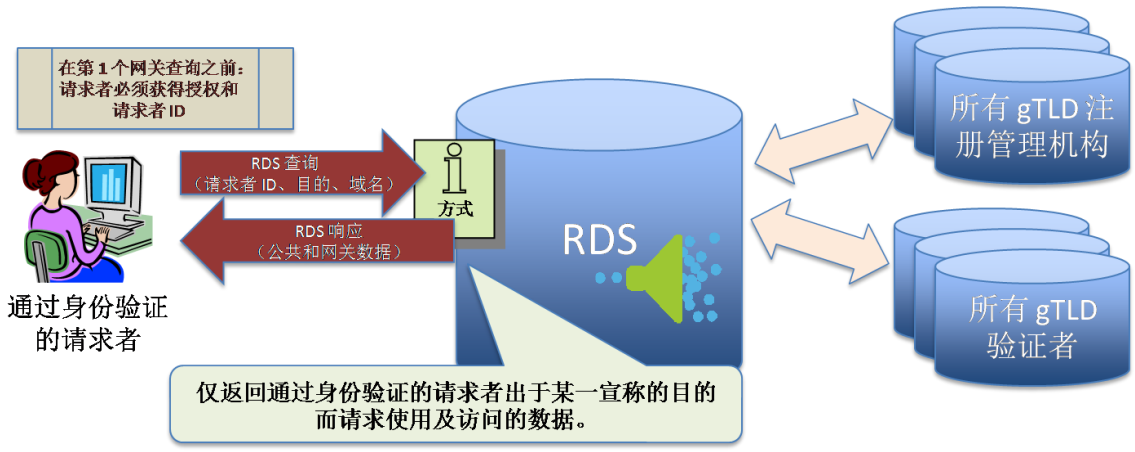


图 7：通过 RDS 对网关注册数据进行访问

技术协议和访问方式

EWG 探讨了在当前域名注册系统中部署技术协议（如，EPP[14]）和在 IETF 中部署技术协议（如，通过 WEIRD 工作组部署）能否为 EWG 建议的设计特性提供支持。目前，WEIRD 工作组即将完成“注册数据访问协议”(RDAP) 这一新标准的制定。在 EWG 建议的模式中应用这些协议可降低所有相关方的过渡成本。

此外，EWG 还分析了 EPP 能否支持建议 RDS 中包含的所有数据元素，以及 RDAP 能否满足 EWG 建议的访问凭证原则这两个问题。分析结果表明，无论最终选择哪种 RDS 模式，EPP 和 RDAP 都能为 RDS 所用。不过，要应用这两者，可能需要进行一些扩展、补充或使用 RDAP“备注”。关于这两个协议的详细评估，请参见附录 G。

c. RDS 用户认证原则

正如第 III 节“目的”所述，某些目的需要访问全部网关元素或经批准的网关数据元素子集。按照第 IV(b) 节原则 #46 的意见，任何需要访问网关数据的目的都必须先通过用户认证。不过，通过用户认证并不意味着可以对网关数据进行无限制访问。所有访问都必须是基于目的的，且仅返回允许所陈述目的访问的数据元素。

EWG 建议，在第 III 节所列 RDS 用户群体出于容许目的请求访问网关数据时，相应的用户认证必须征求群体专家的意见，以确认陈述目的是否属于 EWG 确定的注册数据目的、所请求数据元素对该目的而言是否必需以及是否是负责执行认证的潜在 RDS 用户认证机构。

许多组织都可以与 ICANN 签订合同担任 RDS 用户认证机构这一角色。尽管所有 RDS 用户认证机构都必须遵循一套通用的原则，但 RDS 用户群体不同，适用的实施情况也有所不同。例如：

场景 1：认证机构与认证执行机构并非同一机构，其中，认证机构负责批准用户，但管理经认证用户对 RDS 的访问由第三方执行机构执行

对于商标持有者等 RDS 用户群体，可由行业组织负责对其自己的希望出于容许目的访问网关数据的成员进行认证。这类认证机构可以完全不管用户帐户的管理或 RDS 收到的验证访问请求。相反，它们只负责针对某一给定的 RDS 用户群体制定会员规则、服务条款以及申请和执行流程。随后，该认证机构可以与第三方认证执行机构签订合同，让后者负责创建和管理 RDS 用户帐户、签发 RDS 访问凭证、验证

[14] 请参见 EPP：标准 69，RFC 5730 - 5734

RDS 访问请求以及对滥用行为进行第一级处理，包括暂时停用帐户。认证执行机构的责任仅仅是实施和执行认证机构针对给定群体制定的 RDS 访问规则；任何帐户停用申诉或其他争议都必须呈交给认证机构处理。

场景 2：认证机构和认证执行机构为同一机构，负责将通过身份验证的 RDS 访问请求发送给 RDS

对于 OpSec 等 RDS 用户群体，可由行业组织负责通过它在授予用户访问其他系统权限时所使用的、（经批准的）认证流程对其自己的成员进行认证。这种情况下，该组织同时扮演着认证机构和认证执行机构这两个角色，即，先利用已经被其成员用于身份验证的现有系统执行认证，然后再将针对容许目的的网关访问请求发送给 RDS。如此，RDS 用户必须遵守适用的条款和条件，而该行业组织必须制定相应的流程，用于处理特定用户在访问 RDS 时的滥用行为、帐户停用等问题。

场景 3：认证机构和认证执行机构为同一机构，负责代表其成员向 RDS 提出访问请求（即，Interpol 模式）

对于执法机构等 RDS 用户群体，可由有声望且受信任的组织负责通过它在授予用户访问其他系统权限时使用的（经批准的）认证流程对其自己的成员进行认证。这种情况下，该组织同时扮演着认证机构和认证执行机构这两个角色，即，先利用已经被其成员用于身份验证的现有系统执行认证，然后再代表其成员向 RDS 提出针对容许目的的网关访问请求。如此，该组织会被视为 RDS 用户，其成员所做出的关于代理请求和遵守条款条件的任何行为，一律由该组织负责。鉴于 RDS 可能并不知情用户的具体活动，代理组织必须制定相应的流程，用于处理滥用行为、帐户停用等问题，同时让组织可以对用户的具体访问进行审查和检测滥用行为。

为了让出于容许目的的经认证 RDS 用户能访问网关数据，EWG 建议应用以下 RDS 用户认证原则。

编号	RDS 用户认证原则
56.	必须确保用户能对非网关（即，公共）数据进行实时、无需经过认证和身份验证的访问。
57.	对某些用例和/或请求者而言，对请求访问 RDS 数据的 RDS 用户的认证可以不是实时的。
58.	在决定是否向 RDS 用户提供针对所陈述目的访问网关数据元素的权限时，RDS 只能使用最低要求的“认证方案”。[15]

[15] 例如，这类认证无需采用多因子、宣誓书或无需成为获取大多数类型数据所需的最重要系统。

编号	RDS 用户认证原则
59.	必须无条件地对每一位潜在 RDS 用户进行“预批准”或为其提供凭证。可以针对每“类”经认证的 RDS 用户（即，RDS 用户群体）建立相应的请求和履行流程。
60.	对出于容许目的请求访问数据的 RDS 用户的认证有三种方式。 • 无（即，如上所述，在未经身份验证的情况下仅访问公共数据）。 • 请求数据的个人/实体执行自我认证，例如，某一系统的用户仅陈述了他们的身份、他们请求访问的数据以及请求理由，随后便被授予访问该级别数据的权限。例如，对注册人而言，他们可能需要访问自己的域名数据以实施域名控制，这种情况下，他们在实际注册域名时便已实现了自我认证，从而使得他们有资格获得凭证，对 RDS 内的相应信息进行访问。 • 由某一可信第三方执行认证（即，RDS 用户认证机构，参见下文的原则 #64）。
61.	任何第三方 RDS 认证流程应尽可能利用第 III 节中认为需要获得凭证的各个 RDS 用户群体内已有的认证流程。
62.	负责实施和执行 RDS 用户认证政策的权威机构（如，ICANN、多利益主体专家组）必须定期对这些第三方认证流程进行审查和审核。
63.	任何担任 RDS 用户认证机构的组织都必须与 ICANN 和/或 RDS 提供商签订协议，并按协议规定的准则提供这类认证流程，以及建立可确保正当程序、问责制、安全性、访问的公平性和不违背适用法律的框架。
64.	认证机构可以包揽以下任意一项职责或同时包揽两项职责。 • RDS 用户认证机构可负责定义和管理用户群体，包括建立会员标准、设立获得凭证的要求以及定义并执行其自己的会员条款和条件。 • RDS 用户认证执行机构可负责为认证机构提供平台及相应的平台功能，如用户帐户创建、凭证签发、停用和撤销、用户帐户的生命周期管理以及争议处理和 ToC 执行等相关流程。 认证机构可以但不需要同时包揽这两项职责。

编号	RDS 用户认证原则
65.	希望代表其成员处理 RDS 数据请求的认证机构可以通过以下两种方式来达到这一目的： • 认证机构可通过他们自己的身份验证系统对 RDS 进行代理访问，但需为这一行为承担全部责任。尽管认证机构将对滥用行为负责，但通过认证机构进行代理的请求必须接受身份验证，让认证机构能对个人用户的访问进行审查和解决滥用投诉。 • 认证机构可通过他们自己的身份验证系统提供 RDS 访问权限，不过这仅仅是将经过身份验证的请求转发给 RDS 而已。这种通过认证机构转发的请求必须能对 RDS 用户进行唯一标识，该用户将为这种使用负责，并且直接对滥用行为负责。
66.	根据第 IV(b) 节“原则 #50”的要求，RDS 必须为获得凭证的请求者提供实时访问，提供方式有多种。请求者提出的请求可以由适当的认证执行机构进行身份验证，但在认证期间签发的 RDS 访问凭证必须适用于所有已定义的访问方式。[16]
67.	可定义凭证管理最佳实践；认证机构必须遵守这些最佳实践。
68.	对于验证访问，RDS 必须要求提供个人凭证。
69.	经身份验证的 RDS 访问不具有传递性（即，通过身份验证的 RDS 用户不得与未经过认证的其他人共享网关数据）。
70.	必须建立并执行网关数据的负责任披露流程，以便在最初所请求目的的基础上挖掘更深入的目的。（例如，使调查商标侵权的知识产权所有者能提交 UDRP 投诉，使调查潜在犯罪活动的 OpSec 用户能通知法律的实施。）
71.	希望访问 RDS 数据的组织可以申请 RDS 用户认证，并且在获得认证后可以让该组织内的所有成员都使用 RDS。[17] 不过，这类组织必须负责对内部经认证的访问进行管理。一旦经认证的 RDS 用户组织内存在成员滥用系统的情况，将会导致整个组织受到处罚。
72.	担任多个不同职能的单个 RDS 用户可能拥有多个凭证，以便为达到不同目的而访问不同类型的数据。不过，从可用性的角度而言，只要某一 RDS 用户陈述的每个目的均在第 IV(b) 节定义的目的范围内，便可向该用户提供一份可用于多个目的的凭证，这是非常可取的。
73.	为了检测系统滥用行为和鉴定访问凭证，必须执行审查和数据分析。

[16] 在进行身份验证时必须对验证界面加以定义。例如，对于某些认证方式，RDS 可使用安全声明标记语言 (SAML) 等标准框架，以便负责签发凭证的认证执行机构同时能执行身份验证。

[17] 是否要确保任何已签发 RDS 访问凭证的完整性完全由组织自己决定。

编号	RDS 用户认证原则
74.	必须建立相应的申诉流程，使 RDS 用户能在努力获取/恢复 RDS 访问凭证时对滥用指控进行反驳。
75.	每个注册人必须获得凭证，以便对他们自己的联系人数据进行检查，这些数据存储在 RDS 内，与注册在他们名下的域名相关联。（请参见第 III 节，“域名控制”目的。）
76.	必须建立用于添加其他 RDS 用户认证机构的流程，旨在作为当前流程的补充或提供新颖、创新的用户认证方式。这类 RDS 用户认证机构必须满足本报告所列原则中描述的最低要求。

d. 问责制的主要益处总结

对网关数据元素实行经认证访问是下一代 RDS 的一个重要部分，它要求访问较敏感数据的请求者必须表明自己的身份，陈述自己访问数据的目的，从而可以加强问责制。具体而言，采用 EWG 建议的数据元素和访问原则可带来以下好处。

- 建立以目的为导向的数据收集和披露模式，提高出于容许目的使用注册数据的实体的负责任程度。
- 提供一种支持框架，使数据访问符合不同辖区内的数据保护法。
- 建立一种可向因各种目的访问数据的人追究责任的方法。这可以进一步促进人们遵守不同辖区内的数据保护/隐私规定，同时在负责提供准确数据的人与出于已批准目的使用这些数据的人之间实现问责制的平衡。其中后者有助于消除当前 WHOIS 系统中存在的不公平现象，即数据请求者对访问和使用联系人数据不负有任何责任。
- 使注册人和联系人能更清楚地了解收集注册数据的目的，同时为他们提供更大的自由裁量权，可决定哪些个人信息公开、哪些个人信息封闭。
- 通过提供基本的公共数据集来满足公众访问注册数据的普遍需求，同时减少默认情况下处于公开状态的数据，对访问网关数据的请求者进行身份验证。
- 有助于保护敏感数据元素不被公开披露，让注册人和 PBC 更愿意分享准确性更高的数据，从而提高数据的准确性。除恶意使用以外，一般情况下，若基本的感知风险得以减少，则一旦数据能得到保护、不用向普通大众公开，数据主体往往会提供更为准确的数据，因为这样也可为主体自己带来好处。
- 新增了可选数据元素，便于通过新的或替代的通信方法进行联系，从而提高了 RDS 用户和注册人沟通的整体灵活性和效率。

- 支持通过中央门户网站进行反向查询和 WhoWas 查询，使搜索所有 gTLD 注册数据变为可能，不过这仅限于经认证的 RDS 用户用于容许目的。
- 增强访问功能，提高“系统”的整体效率。
- 提供两种访问：在未经过身份验证的情况下对公共数据进行访问以及通过认证凭证对网关数据进行访问，可消除当前 gTLD WHOIS 响应系统中存在的访问功能、服务级别和格式等混乱，并且允许通过单一标准轻松进行自动化 RDS 查询。
- 提供优质服务和负责任访问，使分布于整个生态系统中的各种防滥用措施得以撤销。

为了实现上述这些好处，必须对 RDS 用户开展关于容许目的和合理使用从 RDS 中检索到的数据的培训，这一点至关重要。此外，寻找愿意负责批准其群体成员访问 RDS 的认证机构可能比较困难。在实施的最初阶段，用户可能会对识别适当的认证机构感到困惑，尤其是对出于多个目的访问不同 RDS 数据的用户而言。而且自动化 RDS 查询也需要更新工具。这些都是建立以目的为导向进行访问的必要初始投资，尽管充满挑战，但会给后续工作奠定坚实的基础，确保 RDS 用户负责任地使用注册数据。

V. 提高数据质量

EWG 建议对注册人数据采用极其严格的验证方式，要比当前 WHOIS 系统所提供的或可通过广泛实施 2013 RAA 加以改进的验证更为严格。首先，注册人应大大改进自己提供的 PBC 信息，使出于各种目的的请求者能根据这些信息联系到相应的联系人，同时采取激励措施，促使注册人提供准确的 PBC 联系信息。第二，对较敏感数据实行网关式访问，使注册人缺少提供错误数据的动机，提高他们对数据准确性的负责任程度。

为了达到这些目标，EWG 提出了两条相关但独立的改进措施：

- RDS 必须对所有 gTLD 注册数据执行标准验证。除定期检查以外，还必须在数据收集时进行验证，同时也可以选择对联系人数据块进行预验证以便在多个域名注册中重复使用。
- RDS 生态系统中必须包含一个经预验证的联系人目录，该目录与域名目录存在概念上的区别，旨在提高数据元素的质量和可重用性以及防止对个人数据的欺诈性使用，其中，此处的数据元素是指用于联系域名注册人及其指定为 PBC（即，可以出于与某一域名注册相关的各种目的与之取得联系）的个人或组织的数据。

关于详细介绍这些建议的原则和流程如下文所述。为了最大限度地获益，EWG 建议同时实施上述两条改进措施，但需注意的是，加强验证对创建联系人目录而言并非必要条件，反之亦然。

a. 数据准确性与验证原则

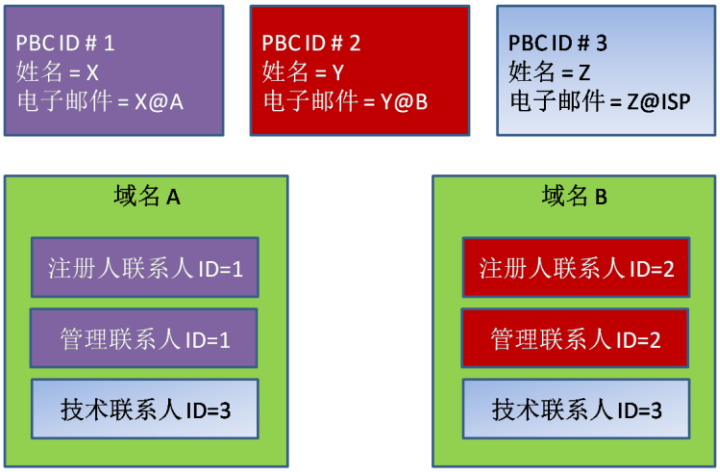
对注册人或其他联系人的信息进行预验证的目的在于：

- 通过利用预验证在发布联系人信息供新域名使用前对该数据进行检查，从而提高联系人信息的准确性，以及使所有域名注册中的数据更一致（减少错误和欺诈）；
- 避免重复验证。在实行预验证之后，只需执行一次验证，后面便可以在多个域名注册中重复使用该联系人数据块，而无需在每次注册人注册一个新域名时都要对注册人或其他 PBC 联系人数据进行验证；以及
- 鉴于验证必须和注册同时进行，实行预验证可避免给域名注册流程带来延误。

服务提供商、法律代表和其他第三方往往是许多注册人名下域名（通常有几百到几十万个域名）的各种问题首要联系点（如，技术、计费、滥用、法律程序）。

为了在这样一个多元化空间中提高数据的准确性和联系人的易用性，ICANN 可以建立适当的机制，使这些联系人可以为多个注册人所用；例如，网站托管商提供自己 NOC 的唯一 ID 作为其客户名下域名的“技术”和“滥用”联系人信息。此外，当这类实体需要更新其联系人信息以反映新的地址/电话号码或资产合并/收购时，如果只需执行一次更新操作，与该联系人数据集（由唯一标识符标识）相关的所有域名都会显示相应更新的话，这应该是非常方便的。

下图描绘了基于目的的联系人 (PBC) 在经过创建和关联到唯一标识符 (PBC ID) 之后，在多个域名注册中重复使用的过程。正如第 III 节所述，PBC 不一定代表个人，而是指联系人持有者明确创建并公布、负责与出于各种 DNS 相关目的的请求者进行联系的联系点。



对 PBC ID # 3 所做的更新
会自动在域名 A 和 B 的
注册数据中反映出来

编号	联系人 ID 及相关数据的原则
77.	联系人管理必须能够与域名管理分开进行，这样，联系人的可移植性和责任追究也就与域名无关，仅受这类联系人下方列出的实际个人或实体的控制。
78.	联系人的管理必须通过验证方执行，它们负责管理联系人数据库、执行验证流程和维护联系人及其数据元素中的有效信息（可通过 RDS 访问）。[18]
79.	域名注册可以与注册人指定的联系人 ID 相关联，并由这类指定联系人（即，可以出于与域名相关的各种目的与之取得联系）进行批准。
80.	这类联系人必须包含有效的强制性数据元素。必须针对这些流程制定相应的政策和实施监督管理，确保联系人 ID 满足最低标准，且没有人在未经联系人授权的情况下使用联系人 ID。
81.	联系人信息的变更管理和使用授权由联系人持有者控制，一旦变更或授权，与该联系人相关的所有域名都将受到影响。因此，必须制定适当的流程和政策，确保在不给 PBC 或注册人带来负担的前提下实施准确、真实、及时的变更，从而为这一新模式提供支持。
82.	每个联系人数据块都必须拥有可唯一标识验证方和联系人持有者的联系人 ID，以便检索和更新相关的联系人数据。该联系人 ID 必须发布在任何公开显示 RDS 数据的位置。

[18] 注：注册服务商可以也有可能成为经认证的验证机构，以便为与他们自己注册的域名相关的联系人提供验证服务。

b. 预验证流程

为了满足需求，EWG 建议采用以下预验证流程：

a) 申请人通过自己选择的验证方（如，注册服务商、注册管理机构、经认证的第三方联系人管理提供商）提交联系人数据。

b) 验证方对语法和操作性进行验证（依据 SAC-058）。

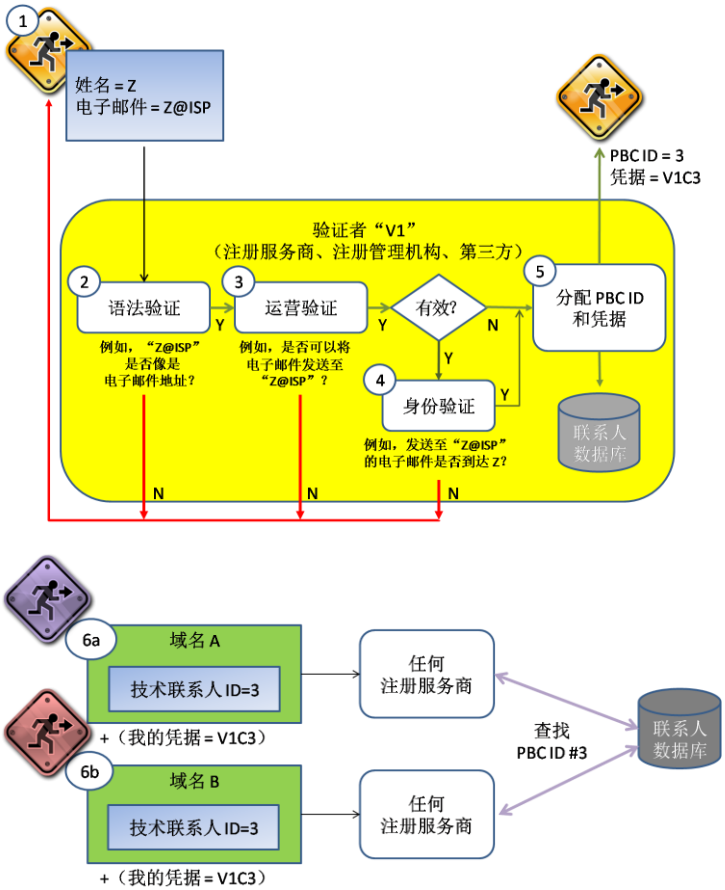
c) **可选**：验证方可利用邮局、ccTLD 管理机构、电话公司、税务局等实体对联系人的身份进行验证，但*需注意两点：一旦联系人符合身份验证标准，则在联系人状态中可注明这一信息以提高用户信任度，进而促进在线业务的发展；这类增值服务会有相应的成本，这些成本将由请求执行这种额外验证的实体承担。*

d) 在成功通过语法验证和所有必需的操作性验证后，验证方将授予联系人数据块（联系人）一串标识符，用于对验证方和联系人进行唯一标识，从而使后续的检索和更新变为可能。

e) 验证方将联系人数据存储在自己的数据库中、签发凭证（如适用，目的在于将来可以对联系人进行更新）以及将唯一标识符转发给申请人（从此处开始，申请人也称为“联系人持有者”）。

f) 联系人持有者将此联系人 ID 提供给注册人，注册人随后可利用唯一标识符将其继续提供给任何注册服务商，并将联系人 ID 作为指定基于目的的联系人（即 PBC）使用来注册域名。*正如第 III 节所述，必须制定和实施相应的授权流程，确保注册人和指定联系人在 PBC 将收到的关于各个域名的目的上达成一致意见。*

g) 在符合第 III(e) 节中基于目的的联系人原则的前提下，可将通过验证的联系人 ID 指定为域名的 PBC（如，注册人、技术、管理、业务、滥用、法务、隐私/代理服务提供商）。



请注意，各个验证方有责任维护自己的联系人数据库。同时，该数据还必须提供给 RDS，但 RDS 模式不同（如第 VII 节所述），具体的提供机制也不同。例如，对于同步模式，联系人数据的补充和更新内容可通过 EPP“推”到 RDS 中。对于联合模式，RDS 可通过 RDAP 实时地将联系人数据“拉”进来。

c. 准确性、审查和补救流程

EWG 建议实施以下流程，确保注册数据持续准确，并对错误的注册数据进行补救：

a) **自我纠正**：联系人持有者让验证方使用验证方之前签发的凭证纠正/更新持有者的数据。利用该特定联系人（由唯一联系人 ID 标识），所有域名内的相应信息都会得到自动更改。

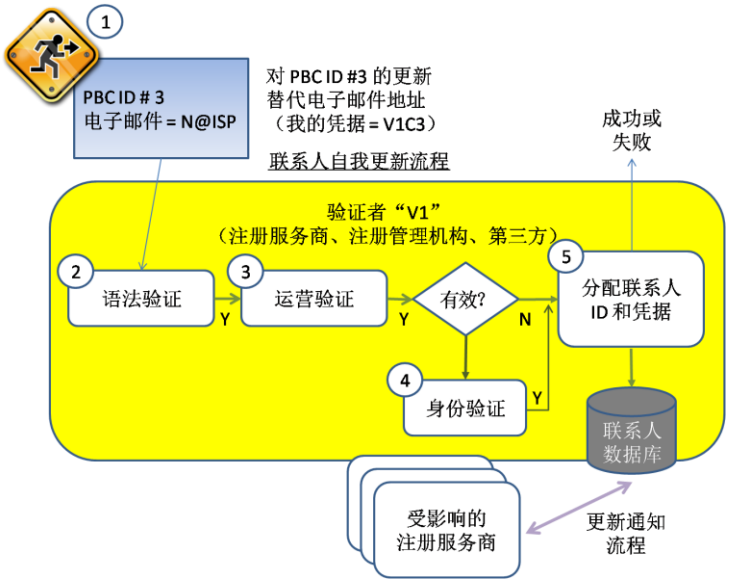
b) **监测流程**：验证方定期对通过自己服务管理的联系人集进行操作性验证和非必需的身份验证。*注：这类验证流程不应过于繁琐，一旦执行了验证，便可在相应联系人的状态中加以说明和反映（例如，联系人的可操作性于 2016 年 1 月 1 日前有效）。*

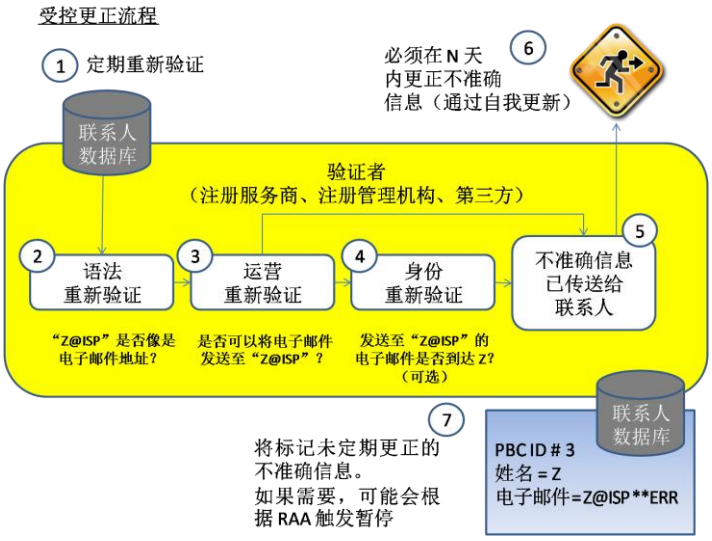
c) 一旦检测到任何错误数据，验证方将其报告给联系人持有者，并规定联系人持有者在某一特定时间段内（例如 14 天）予以纠正。同时，验证方可以通知任何受影响域名的注册人、注册管理机构和注册服务商这一事件。随后，联系人持有者让他们之前选择的验证方通过验证方签发的凭证对错误数据进行纠正。

d) 如果在上述时间段结束后注册数据仍未得到纠正，则该数据将被标记为“错误”。如果被标记数据对当前引用此联系人 ID 的任一 PBC 而言属于强制性数据，则相关域名将进入补救流程，即通知错误数据所属的注册人，让注册人在 RAA 规定的时间段内对数据进行纠正。未在规定时间内完成纠正的域名将受到制裁，按照适用 RAA 的规定，这一制裁可能包括域名停用或删除。

e) 一旦注册人将被标记数据替换为有效数据，对相应域名的任何制裁便不再适用。

f) 若验证结果不符合 ICANN 规定且已向 ICANN 合规部门提交准确性报告，则验证方将收到重新验证语法和操作性的通知。重新验证成功的，提交准确性报告的当事方可针对自己的情况再采取其他适当行动（如，提交 UDRP 投诉或提交披露请求）；重新验证失败的，必须通知使用该错误联系人 ID 的所有域名的注册人，要求他们执行上述正常补救流程。





d. 联系人 ID 的运作机制

EWG 建议采用以下机制来管理联系人 ID 以及将联系人 ID 与注册信息进行关联：

a) 所有验证方验证的联系人 ID 都必须具有唯一性，以确保联系人 ID 的可移植性以及在域名和必要目录信息之间提供明确的映射。

b) 为实现数据检索和更新，用于标识联系人和验证方的联系人 ID 必须与分散的联系人数据块相关联。说明：一个联系人 ID 必须映射到一组联系人数据，这些数据是用户联系指定域名联系人所必需的。如果所提供信息不满足这一要求，则就可操作性而言毫无用处。

c) 联系人 ID 必须由经认证的验证方分配。任何实体均可申请成为验证方，申请标准与现在用于认证注册服务商的标准类似。经认证的验证方既可以是注册服务商、注册管理机构，也可以是第三方验证提供商。理由：验证方是创建联系人数据库所必需的职能机构。尽管针对不同联系人的验证级别可能有所差异，但不同验证方使用的验证流程必须统一，这样才能确保准确性，确保对域名注册人及其指定联系人负责。

d) 为了实现与域名之间的关联，注册人或指定 PBC 必须获得联系人 ID。

e) 联系人 ID 可分配给一个或多个域名的多个角色。例如，某一给定 PBC ID 对某一域名而言是注册人 ID，而对其他域名而言则是技术和滥用联系人。

f) 任何时候均可创建和修改联系人，包括在域名注册流程中创建和修改。

e. 与验证方的互动

EWG 建议验证方与联系人持有者（即，所创建的联系人数据块成功通过验证且可重复使用的当事方）遵照以下原则进行互动。

编号	联系人持有者与验证方的互动原则
83.	对于任何给定联系人 ID，联系人持有者可选择任意验证方进行验证[19]。
84.	必须制定用于管理联系人 ID 的监督和问责政策。
85.	必须确保联系人持有者能通过负责签发凭证的验证方对与联系人 ID 相关的联系人信息进行修改。
86.	验证方必须对联系人持有者进行身份验证，防止他人对与联系人 ID 相关的联系人信息进行未经授权的修改。
87.	验证方可以对联系人持有者执行多种不同级别的身份验证，包括从基本的 PIN 验证到双重验证。必须确保联系人持有者能够根据成本效益定位来选择验证提供商，包括易用性、安全性、成本和其他逻辑业务因素。
88.	验证方必须公布其身份验证政策，且该政策必须能供全球用于声誉管理。此举将有助于提高所列联系人信息的准确性和加强关于这些信息的问责制。
89.	验证方必须具备验证以联系人持有者母语提交的联系人信息的能力。这有助于提高母语数据的准确性，同时为将域名注册系统扩展至多语言环境提供支持。例如，注册服务商可以与不同地方的验证方合作，为大量注册人和指定联系人提供扩展的验证服务，无需投资昂贵的工具便可对用工作人员不熟悉的语言提交的数据进行验证。

[19] 根据原则 #88 的描述，联系人 ID 用于标识验证方和联系人持有者。因此，持有者在选择验证方时应确保联系人 ID 在不同验证方之间可移植。

f. 联系人验证原则

根据 SAC 058 的规定，联系人数据的验证可分为三个级别：语法、操作性和身份。EWG 建议实施以下验证原则。

编号	联系人验证原则
90.	所有与联系人 ID 相关联的联系人数据元素都必须经过语法验证。这是行业内所有实体均有能力达到的基本验证级别。
91.	所有与针对某一特定目的的联系人 ID 相关联的强制性联系人数据元素都必须经过操作性验证[20]，只有通过这一级别的验证后，该联系人 ID 才能纳入针对该目的的域名注册数据中。
92.	联系人持有者可主动要求执行非必需的更高级别验证（如，可选的身份验证），但需承担因此产生的费用，当然也有一定的好处（如，消费者对注册在经身份验证的实体名下的域名往往更有信心）[21]。
93.	鉴于可选身份验证服务的收费不低，ICANN 可以提供一种低成本机制，为处于经济弱势的联系人持有者进行可选身份验证提供支持。
94.	为了可以在保持关联性的同时对数据进行修改，可将联系人 ID 的状态设为“错误”，ID 仍然留在系统内。
95.	适当情况下，在访问 RDS 信息时，必须追踪并发布联系人 ID 的验证状态，以及最近一次确定验证状态的时间。
96.	如第 V(c) 节所述，在对某一联系人 ID 的验证状态存有质疑时，第三方可提出错误报告，这将启动标准补救流程，结果可能是该联系人 ID 被标记为“错误”，进而给将该联系人 ID 作为 PBC 使用的域名带来后果。
97.	活跃域名的强制性联系人在被标记为“错误”状态后，必须采取某种补救措施。不过，具体的补救流程可另外确定。
98.	在跨域验证适用的情况下（如，实际地址），必须对与联系人 ID 相关联的所

[20] 欲了解操作性验证和当前 ccTLD 实践的可能实施方式，请参阅 SAC 058 和 *ccTLD WHOIS 数据验证调查结果概览*。

[21] 例如，可选的身份验证既可以作为单独收取费用的增值服务提供，也可以捆绑到域名注册服务包中，还可以作为对大客户的激励进行提供。请参阅*联系人数据验证 RFI 与验证系统*，了解更多关于执行此类验证的商业服务示例。

编号	联系人验证原则
	有联系人数据元素的最低跨域验证级别进行检查。
99.	适用验证方必须定期对联系人数据进行重新验证，确保所公布的数据准确。
100.	如联系人持有者提供有可选的数据元素，则这些元素必须至少经过语法验证。除此之外，除非联系人提出请求且有能力支付验证产生的所有费用，否则不会对这些元素进行其他验证。
101.	如果数据元素接受了除语法验证以外的其他级别验证（操作性验证或可选的身份验证），则验证方必须对这些验证加以记录并维护。例如，对电子邮件地址、电话号码和地址这类元素的验证属于操作性验证，而对姓名或所在组织名称的验证既可以是操作性验证，也可以是身份验证。
102.	此外，验证方必须决定各个联系人 ID 获得的整体验证状态，并将该状态作为一项 RDS 数据元素进行发布。例如，若接受操作性验证的所有强制性数据元素均通过了相应的检查，则联系人的整体验证状态为“通过操作性验证”；一旦其中有任何强制性数据元素未通过检查，则联系人的整体验证状态将降级为“通过语法验证”。若接受身份验证的所有强制性数据元素均通过了相应的可选检查，则联系人的整体验证状态将升级至“通过身份验证”。为了提高数据准确性和沟通效率，该整体验证状态必须作为各联系人的新增数据元素向 RDS 用户提供。[22]
103.	对于任何经过验证的数据元素，验证方必须记录并维护相应的验证时间戳。
104.	验证方必须决定某一整个联系人 ID 最近一次变更整体验证状态的时间，并将其作为各联系人的新增 RDS 数据元素进行发布。

g. 唯一联系人数据的作用

为了防止假冒、诽谤和滥用，联系人持有者可将自己的联系人数据标识为唯一联系人数据，禁止其他申请联系人持有者的人使用。

a) 唯一联系人数据可包含某一联系人集的多项元素，尤其是电子邮件地址和电话号码。不过，地址和姓名的唯一性可能很难甚至无法保证。

[22] EWG 也考虑过发布注有每项联系人数据元素获得的单项验证状态的 RDS 数据元素，例如，PBC 电子邮件地址状态 = 通过操作性验证、PBC 名称状态 = 通过身份验证。不过，按照这种粒度发布验证状态需要大量的协议、数据元素和客户端应用/GUI 变更，因此现阶段不建议这种做法，但它值得进一步研究。

b) ICANN 必须建立适当的机制，使其他验证方在某一联系人持有者申请唯一性标识时，能够对比该联系人持有者申请的联系人数据集与自己持有者申请的数据集，确保新联系人 ID 的申请人（或修改联系人信息的现有联系人持有者）不会涉及侵犯受唯一性保护的数据。[23]

c) 任何标识为唯一的数据都必须接受身份验证，以防假冒和“拒绝服务”式攻击（合法联系人无法使用他们自己的真实数据）。

h. 提高数据质量的主要益处总结

在下一代 RDS 中纳入联系人 ID 管理和验证系统将使得注册人难以向 RDS 内填入虚假数据，以及有助于减少欺诈行为和身份盗窃行为，从而提高数据质量。具体而言，采用 EWG 建议的数据准确性和验证原则可带来以下好处。

- 提高个人、组织控制和维护自己联系人数据的能力，无论这类数据在域名生态系统中的哪个位置使用，个人和组织都可以进行控制和维护。
- 鉴于所有联系人在创建或更新时必须经过最低级别的验证，这使得恶意者难以获取域名。验证方的认证要求应能识别和处罚不符合运营标准的恶劣验证方或不严格的验证方。一旦通过单个域名注册发现恶意者，则该恶意者持有的其他域名也可能因共用 PBC 而被发现和处理。
- 若某一给定注册人注册了多个域名，则采用这些原则可提高域名数据的一致性。尽管可能存在联系人验证等一些前期成本，但经验证的联系人 ID 具有可移植性，可完美地移植到其他域名注册中，而且应该能大大减少许多注册人将来的维护成本。
- 提高检测无效联系人信息和利用该信息修复整个域名集的能力。验证方的定期验证或更新验证要求应强调过时联系人信息的问题，并且能在一次更改后自动将更新应用于所有受影响的域名注册。
- 降低整个生态系统的成本，提高整个生态系统的效率。尽管引入联系人管理会增大整个注册系统的复杂性，但联系人管理可与域名注册管理分开进行，这既实现了联系人数据管理的本地化，又可以对域名进行大规模更新。
- 使服务提供商能够对联系人详细信息进行无缝更新，而无需对将这些联系人作为基于目的的联系人的域名注册进行单独更新。对许多提供商而言，这意味着可以轻松更新数千甚至数百万的域名。

[23] 此唯一性检查在同步 RDS 模式下较为容易，在联合 RDS 模式下可能比较困难。

- 提供可选的身份验证，有助于减少假冒注册数据带来的滥用行为。尽管要求可选身份验证的联系人持有者可能需要承担相应的费用，但一旦通过身份验证，便能够有效遏制如今经常发生在高调实体、大型服务提供商或遭到恶意攻击的个人身上的假冒（身份盗窃）滥用行为，因此，此举是非常值得的。
- 联系人数据管理和验证与域名注册/管理分开后，数据主体与其数据可以更贴近，在选择验证方时便无需顾及注册服务商或注册管理机构的所在地，而选择联系人持有者当地辖区内的验证方，从而有助于更方便地应用相关数据保护法。
- 验证方能够用联系人持有者和注册人的母语向他们提供服务，从而提高数据质量和准确性，并因此降低验证成本。而且，这使得注册服务商能够用他们不熟悉的语言提供服务，或通过分布式的验证方对自己的数据进行验证。

VI. 法律和合同注意事项

EWG 的工作一直以一些首要的法律原则为指导：

个人数据必须： • 以合法、公平以及与数据主体相关的方式透明处理； • 收集以用于特定、明确和合法目的，不以与这些目的不符的方式进一步处理； • 适合它们的处理目的、与其相关并且仅限于满足最低要求；并且 • 根据需要保持准确和最新状态，以用于指定目的。
可以根据以下条件进行合法处理（包括传输和披露）— 受相关管辖区约束： • 数据主体是否同意； • 履行数据主体是其一方的合同的必要性；以及 • 遵守管理者受其制约的法律义务的必要性。
必须确保数据主体访问信息的权利和纠正不准确信息的权利。

EWG 建议，在为 RDS 起草最终政策和实施流程时，应考虑数据保护法通常规定的这些以及其他相关原则。此外，各方公认在一些管辖区，在言论和结社自由方面，隐私权将扩展到法人和实体。EWG 认可这两类在全球分别以不同方式加以保护的不同权利。

在此基础上，EWG 评估了相关方案，然后为隐私和数据保护以及执法部门访问制定了 RDS 原则。本部分将介绍那些 EWG 原则，合同合规性、问责制和审核原则将为它们提供支持。

a. 数据保护原则

目前，声称满足隐私和消费者保护方面的可适用国家法律的做法并不一致。一些法律规定，在将数据导出到受该法律监管的个人或数据处理者的管辖区以外时，应采用类似或同等的数据保护。除非本地法律评估认为“适当”，否则欧洲 1995 年数据保护指令禁止将数据传输到该管辖区以外。欧盟以外的许多其他管辖区已制定了严格的合法条款，但无论如何，大多数法律均规定，除非保证提供保护，否则持有个人数据的一方不得将其传输或披露给其他方。这种传输可能会产生法律责任。当前，ICANN 通过在 RAA 合同中向证实其遵守禁止数据托管的数据保护法的注册服

务商提供豁免权，解决了这方面的问题。这不是 ICANN 生态系统内唯一会给那些寻求遵守数据保护法的组织造成风险的条款，因此，人们一直建议需要对现状进行仔细分析。鉴于 EWG 的工作一直以问责制为重点，因此已经考察了负责数据保护方面的要求。

目前，必须根据**具体情况**满足一些要求，即接收个人数据的实体必须保证提供充分并且与提供给“在国内”的数据主体的保护相一致的保护，具体取决于接收数据的实体是处在提供法定数据保护还是类似充分保护的管辖区。这意味着，将实施由适用于接收数据的实体的法律确保的充分保护或其他保证，以便依据适用于数据主体的法律，数据传输是合法的。

数据保护机制

根据当前的情况，共考察了四种用于保护整个 RDS 生态系统内的个人数据的渐进式方案：

(0) 什么也不做；

(1) 引入促进例行进行合法数据收集和传输的机制；

(2) 引入各种机制，寻求在整个 ICANN 生态系统内协调隐私和数据保护，并提供基本的数据保护“平台”，以确定公认的隐私政策最佳实践；以及

(3) 作为一组“约束性公司规则”提交上述政策。

> **注：**在本部分，“RDS 生态系统”是指第 VIII(c) 部分“合同关系和合规性”和第 VIII(d) 部分“问责制和审核”中列出的所有参与方。这包括 ICANN（一家美国非盈利机构）、所有 gTLD 注册管理机构和注册服务商（每个机构均作为独立公司在许多国家或地区运营），以及 EWG 在本文档中提议的所有新委任实体：RDS 提供商、验证方、安全保护凭证批准方、RDS 用户委任方、ICANN 合规部门，以及参与处理个人数据的任何其他实体。

方案 (0)：“什么也不做”

由于不遵守数据保护法的风险继续增加以及需要研究每项注册来确定可适用的法律，什么也不做将导致非常高的复杂性。对某些运营商，特别是注册管理机构来说，这会造成非常大的开销。对注册服务商来说，这需要付出高昂的成本来监控注册人和注册管理机构所需保护的充分性。这会增加所有相关方（包括 ICANN 和域名系统中的其他利益主体）的法律不确定性。gTLD 数量的增加和注册管理机构站点的多样性会给 ICANN 的合同制度带来有关可适用法律和管辖区方面的新挑战，因为它们与注册人隐私和消费者保护有关。混乱、不确定因素以及不一致的做法需要

ICANN 付出更大的努力来确保合同合规性并降低潜在的风险。即使没有 RDS 问题，这些挑战也会存在。引入了 1000 多个 gTLD 后，问题变得更加严重。更重要的是，无法始终保证为数据主体提供保护。建立一个降低风险、最大限度减轻负担以及减少复杂性的协调框架符合每个利益主体的利益。

方案 (1)：引入促进例行进行合法数据收集和传输的机制

考察的第二个方案是引入一个系统，用于评估相关隐私和数据保护法，并在列表中列出相关法规，以便利益主体应用它，个人可以了解他们数据的位置以及哪些法律适用。RDS 可以通过在下一部分定义中的“规则引擎”自动应用该列表。如果某个人居住在实施数据保护法的国家/地区，并且相关法律适用于在该国家/地区以外此个人传输给另一方（此处为注册服务商）的个人数据，则该法律可能适用。如果注册服务商位于其数据保护法适用于所有个人（即不仅包括它自己的公民）的国家/地区，则该法律当然适用。存在疑问或在我们目的范围内的数据仅为那些在 RDS 中收集的数据[24]。对生态系统中应用的相关管辖区数据进行编码会降低相关利益主体面临的复杂程度，确保注册人的数据保护权利（如果适用），以及降低不合规风险。但是，在没有适用于域名注册企业、注册管理机构或 ICANN 及其合规机制的数据保护法的管辖区，这种方案并不能为个体注册人提供太多保护。这可能导致多层隐私权系统，即一些个体注册人没有隐私权，而其他注册人拥有全部的人权和具有司法监督的诉讼理由。

方案 (2)：引入各种机制，寻求在整个 RDS 生态系统内协调数据保护，以提供基本的数据保护“平台”，确定公认的隐私政策最佳实践。

可以起草合同条款来填补隐私保护中的任何差距（将在实施过程中进一步讨论），这些条款可以基于一组被普遍接受的隐私保护方法，这些方法将构成 ICANN 隐私政策的基础。该政策可能较为简洁，附录中列出了相关条款。这样做可以通过提供级别足够高的数据保护来避免由于个人隐私、数据保护和消费者权利理由而提出反对，从而在 RDS 生态系统参与者之间自由地传输数据。

促进在此 RDS 生态系统中合法进行数据收集和传输的机制可以采取各种形式，但这些机制均应基于适用于该 RDS 的一贯的数据保护政策。ICANN 将通过合同条款向所有利益主体实施该政策，就像它实施所有其他政策一样。

[24] 这不一定会降低注册服务商工作的复杂性，这些服务商控制着大量未传输到 RDS 的敏感数据，如银行数据、信用卡信息、客户服务记录等；但考虑到将来 gTLD 系统的复杂性，在某些情况下，“规则引擎”肯定有用。

方案 (3)：在上述方案 (2) 的基础上，由 APEC 和欧盟隐私/数据保护法确认且可以作为一组“约束性公司规则”提交制定的政策。

此方案将简化 28 个欧盟成员国之间的数据传输，因为它会针对欧盟国家的目的提供充分的数据保护，改变了根据整个 RDS 生态系统中的数据流做出数据保护决定的临时性质。虽然此方案可能会耗用更多时间，但它可以降低不合规风险并确保提供更强大的保护。它还可以为隐私政策提供独立监督。

编号	考量的数据保护机制汇总
(0)	什么也不做。
(1)	最低解决方案将 a) 确定法律可确保为其提供充分隐私保护的传输并公布各自的列表；并且 b) 在合同中为那些传输无法由法律提供充分保护的 RDS 生态系统参与者制定通用规则，从而为合规职能部门提供一个单一而简单的维护平台。
(2)	可以根据隐私保护的标准最佳实践为 RDS 起草基本的 ICANN 隐私政策，并且可以制定在整个 RDS 生态系统内实施此政策的标准合同条款。可以在 ICANN 与所有进行数据传输的 RDS 生态系统参与者之间签订的合同中纳入这些标准条款，确保提供足够高级别的数据保护，以便在此生态系统内进行自由传输。
(3)	将 ICANN 视为一个跨国非盈利性机构，在其控制下的整个 RDS 生态系统可能会受约束性公司规则 (BCR) 的制约，事实证明，这会有效促进在组织内进行全球数据传输。在此情况下，生态系统将成为合规性主体。通过设定政策和合同要求，可以将 ICANN 视为“数据管理者”以使用 APEC 和欧盟术语。

评估：

方案 (0)：什么也不做。考虑到系统的全球复杂性不断增加且工作重点为提高准确性和问责制，这种方案被认为是不可接受的。

方案 (1)：促进例行进行合法数据收集和传输的机制。随着不同管辖区中的法律发生改变，此方案可能会变得更加复杂、更加动态，并且必须考虑生态系统内的复杂数据流。如前所述，某个体注册人的注册服务商在另一个管辖区，使用的验证方在第三个管辖区，维护数据的注册管理机构在第四个管辖区，并且依赖第五个管辖区中的 RDS 提供商。

方案 (2)：努力协调整个 RDS 生态系统内的数据保护的标准合同条款。此方案可能需要遵守声明的利益主体的可适用法律，这些利益主体主要包括注册人、注册服务商、注册管理机构和 ICANN。其中还可能包括此报告中建议的新 RDS 生态系统参与者：验证方、RDS 提供商、RDS 用户委任方等。

除了责令遵守本地数据保护法外，在列举 APEC 和欧盟数据保护法中的常见要素的过程中，此方案会设法确保合规性。通过（例如）合并欧盟有关合法数据处理的要求与约束性公司规则规定的相应要素，相关条款可以指定同意条件、访问权限、保留政策以及其他要素。这些标准合同条款不一定需要数据保护机构授权/监控，处在必须提供此类授权的管辖区的情况例外。

方案 (3)（针对 RDS 生态系统的 BCR）：除了责令遵守本地数据保护法外，此方案可能会列举 APEC 和欧盟数据保护法中的常见要素。如方案 (2) 中所述，通过（例如）合并欧盟有关合法数据处理的要求与约束性公司规则规定的相应要素，相关条款可以指定同意条件、访问权限、保留政策以及其他要素。这些标准合同条款不一定需要数据保护机构授权/监控，处在必须提供此类授权的管辖区的情况例外。但是，必须修改 BCR 以适应 RDS 生态系统的规范。与结构松散的生态系统（如 ICANN 运营的生态系统）相比，BCR 可能更适用于采用传统控制结构的公司实体，但当然，跨国公司会通过与 ICANN 用于委任和控制其利益主体完全相同的合同来实施其约束性隐私规则。

总体而言，“什么也不做”并不是一个真正的方案，特别是在 EWG 旨在提高准确性和问责制的建议被接受的情况下。方案 (1) 在法律上具有相当的复杂性，并且无法为所有注册人提供同等的权利，而方案 (3) 引起了有关 RDS 生态系统内适用性的担忧（即制约性公司规则是否可行，是否会被接受，在法律责任方面会对 ICANN 造成什么影响？）。

因此，EWG 建议采用方案 (2) — 使用与数据保护法相一致的标准合同条款制定一项政策，以落实该政策的要求，并通过各种审核机制确保通过所有参与处理个人数据的 RDS 生态系统参与者之间的合同强制执行这些隐私保护。

实施数据保护机制

对上述所有方案来说，RDS 实施问题都至关重要 — 特别是在 RDS 提供商的本地化方面。

如果 RDS 将持有个人数据，则为了避免与数据传输合法性和数据泄露法律责任相关的问题，这些数据位于提供了可执行的数据保护权利的管辖区会较为方便。如果 RDS 持有常驻并且与数据处理者位于同一地点的数据，则明显存在该问题。即使数据不是常驻数据，而是提交到那里以进行处理（例如验证），然后发送到其他位置，也应该采用类似的考量框架。EWG 考虑了以下三个数据保护实施方案：

编号	考量的数据保护实施方案汇总
(0)	如果在做出地理位置选择时未考虑适用于 RDS 本地化的合法数据保护级别，则“什么也不做”适用。这样做可能会导致管辖区内的 RDS 本地化获得较低级别的数据保护。
(1)	RDS 可能会提供某种法律区分。具体来说，可以根据适用于数据主体（如，注册人）的法律标记数据元素并进行相应处理。为实现这种法律区分，RDS 可以实施一个“规则引擎”，对每个特定的传输应用适用的数据保护法。 更具体地说，“规则引擎”指可以在 RDS 内实施的一项功能，用于 (a) 根据注册人、联系人、注册服务商、注册管理机构和 RDS 管辖区（用以下数据元素表示：注册人和联系人国家或地区代码、注册服务商和注册管理机构管辖区）来管理域名信息的存储、收集和处理，并 (b) 依照 ICANN 将来为 RDS 定义的政策管理适用管辖区的数据保护法。 如上所述，如果 RDS 所在的管辖区不具有可提供向法院申诉权利的数据保护法，则这种做法本质上会非常复杂并且难以执行。
(2)	将根据最简单最不复杂的数据传输标准选择 RDS 的本地化。这样做意味着为 RDS 数据存储选择可适用国家数据保护法提供了高级别保护的地点。

评估：

方案 (0)：“什么也不做”将保持现状并会增加许多数据传输的复杂性，因为它：

- 继续采用一个很难且实际上几乎不可能尊重法律框架的流程；
- 给注册服务商以及生态系统内的其他参与者（包括 ICANN 合规部门）造成了管理和法律责任；并且
- 在本地数据保护法和隐私合规性方面完全不透明而且无法扩展。

方案 (1)：通过“规则引擎”进行法律区分具有创新性，但必须在技术上测试其可行性。在法律上存在许多尚待解决的问题，特别是在定义、法律认可度以及实施此类系统方面。

方案 (2)：在选定管辖区进行数据本地化可能是一个简单方便的解决方案，可为所有数据转移提供非常高级别的保护。但是，此方案本身并不会导致应用每个主体的本地数据保护法。

由于方案 (0) 不可行，方案 (1) 和 (2) 并不相互排斥，*因此，EWG 建议目前应考虑同时采用方案 (1) 和方案 (2)，以实施将通过政策和标准合同条款确保的高级别数据保护。*

在考虑所有这些有关数据保护政策、机制和实施的方案后，EWG 就以下原则达成了一致：

编号	数据保护原则
105.	必须采用促进在 RDS 生态系统内的参与者之间例行进行合法数据收集和传输的机制。
106.	应将与隐私和数据保护法相一致的标准合同条款编写成政策条文，并通过所有参与个人数据处理的 RDS 生态系统参与者之间的合同进行实施。
107.	必须考虑建立一个应用数据保护法的信息系统（即“规则引擎”）以及对 RDS 数据存储进行本地化，将其作为实施所需高级别数据保护的两种方法。必须通过 RDS 生态系统的合理隐私政策中的标准合同条款为上述做法提供保证。

b. 执法部门的数据访问原则

与数据保护不同，在执法部门访问时为数据主体提供的法律保护无法“导出”。在执法部门访问方面，考量了三个方案。

编号	考量的执法部门访问方案汇总
(0)	“什么也不做”。只要国家执法部门有权访问各自国家/地区层面上的每个数据存储库中存储的 RDS 数据，执法部门访问就应遵循现有的规则。在集中化 RDS 门户，将根据 RDS 门户所在国家/地区的国家法律授予访问权限。
(1)	在中央 RDS 门户级别（这里的数据无法公开访问，并且根据适用的国家法律，执法部门在这里不需要特定的法律程序），可以为 RDS 系统指定访问条件并按以下两种方式之一实施这些条件：

编号	考量的执法部门访问方案汇总
	a) 欧洲刑警组织和国际刑警组织可与 RDS 签订合同协议，以实施和执行此类系统，将其作为所有执法部门访问的实时活动媒介，并负责相应的数据保护和使用。 b) 欧洲刑警组织和国际刑警组织可与 RDS 签订合同协议，以充当执法部门群体的用户委任方，审核申请以签发 RDS 凭证，然后，各个机构将使用该凭证访问网关 RDS 数据并负责相应的数据保护和使用。
(2)	此外，可以在中央层面制定一些机制，以便执法部门访问中央 RDS 门户，即使该层面在传统的双边关系方面存在将由《司法互助条约 (MLAT)》处理的特定要求。可适用法律方面的数据区分可为制定此类机制提供支持。

评估：

方案 (0)（“什么也不做”）明显无法为执法部门提供附加访问价值。

方案 (2)（RDS 用户访问门户级别的 MLAT）可通过 RDS 访问的任何建议的网关数据元素将不需要其他司法授权即可供执法部门访问。因此，不需要进一步考量方案 (2)。

方案 (1)（委任的 RDS 用户访问门户方法）便于执法部门进行访问。虽然变体 (1a) 和 (1b) 建立在现有结构的基础之上，但变体 (1a)（通过实时媒介进行区分委任访问）也建立在执法部门合作的现有机制的基础之上，并且可避免增加另一层复杂性。但是，仍然必须确保能够检测和纠正潜在的个人滥用。

第 IV(c) 部分：RDS 用户委任方案 #3 进一步探讨了变体 (1a)，该部分详细说明了潜在委任方（如，国际刑警组织）如何代理针对 RDS 的已授权执法部门访问请求，同时阻止潜在的滥用。请参阅 RDS 用户委任原则了解相关建议。

此外，对于方案 (1)，必须确保在存储 RDS 数据的管辖区为国家执法部门建立的法律框架不会取代为 RDS 建立的框架。因此，RDS 本地化的地理分布非常重要。

编号	执法部门访问原则
108.	RDS 必须将数据存储在执法部门得到普遍信任的管辖区，而不论采用何种实施模型。

c. 合规性和合同关系原则

EWG 为 RDS 生态系统内各方之间的合同关系建议了以下一组原则：

编号	合同关系原则
109.	具有全球规模的非政府组织第三方提供商应运营 RDS。
110.	ICANN 必须与 RDS 第三方提供商签订相应的合同以提供可用性、审核和合规性。
111.	ICANN 必须与验证方、隐私/代理服务提供商、安全凭证批准方以及其他可能与 RDS 交互的相关方签订相应的合同（请参阅第 III(c) 部分原则 #1）。
112.	ICANN 必须修订现有协议（RAA、注册管理机构协议）以符合 RDS 要求并取消原有的要求。
113.	RDS 必须适用于所有现有的或新增的 gTLD 注册管理机构。不允许任何过渡或特别豁免。

d. 问责制和审核原则

EWG 建议，RDS 生态系统参与者应对向注册信息采取的行动负责，如下所述：

编号	问责制和审核原则
114.	RDS 生态系统内的所有实体必须对表 6 中提出的一个或多个要求负责： a) 提供准确而可靠的注册信息 b) 仅将信息用于指定目的 c) 确保所收集、存储和转发的信息的安全性 d) 在收集时对信息进行验证或鉴定 e) 及时更新以前提供的信息 f) 实施 RDS 隐私政策和使用条款 (ToU) g) 检测注册信息的滥用情况 h) 处理和跟踪投诉 i) 遵守制定的 ToU 和 ToS 政策 j) 建立机制来阻止第三方数据收集以及批量创建欺诈性帐户 k) 建立持续的审核和修正流程 以下利益主体[25]在 RDS 生态系统内承担问责制角色： a) RDS 寻找数据的用户 (USD)— 见第 III 部分

[25]这些角色和责任扩展到利益主体代理和受让人（如，分销商）

编号	问责制和审核原则
	b) 注册人 c) 注册服务商[26] d) 注册管理机构[27] e) 注册目录服务提供商 f) ICANN g) 隐私或代理服务提供商 h) 安全保护凭证批准方 i) 验证方 j) RDS 用户委任方 k) 基于目的的联系人 l) 托管提供商
115.	RDS 必须制定程序来处理有关数据不可用、数据误用、未授权数据访问、违反隐私政策以及不准确的数据录入的投诉；例如：滥用联系人数据元素，以及一个用于获取来自 USD 和注册人的投诉的门户。
116.	RDS 必须为不准确数据制定上报补救措施；例如：电子邮件警告、记录上用户/浏览器可见的标志、ICANN 合规行动，以及鼓励提高准确性的其他新激励措施。（请参阅第 V 部分“提高数据质量”了解准确性要求。）
117.	RDS 必须为未授权数据访问制定上报补救措施；例如：电子邮件警告、速率限制、临时阻止、暂停委任、解约和其他遏制措施。（请参阅第 IV 部分“加强问责制”了解网关访问要求。）
118.	RDS 必须为数据误用制定上报补救措施；例如：电子邮件警告、速率限制、临时阻止、暂停委任、解约和其他抑制措施。（请参阅第 III 部分“用户和目的”了解容许目的。）
119.	RDS 必须建立审核机制来检测对 RDS 访问凭证的滥用和 ToU 违规行为；例如：用于检测不同寻常的行为模式的机制。（请参阅第 IV 部分“加强问责制”了解 RDS 用户委任要求。）
120.	RDS 必须建立审核机制来检测滥用注册数据以用于非指定目的的情况；例如：用于检测不同寻常的行为模式的机制。（请参阅第 III 部分“用户和目的”。）

[26] 如 http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm 所定义

[27] 如 http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf 所定义

编号	问责制和审核原则
121.	RDS 必须建立审核机制来检测验证方的滥用情况；例如：验证方培训、定期对要检查的数据进行随机抽样以确保正确进行验证。（请参阅第 V 部分“提高数据质量”。）
122.	RDS 必须建立审核机制来检测 RDS 用户授权方的滥用情况；例如：建立用于检测不同寻常的行为模式的机制。（请参阅第 IV 部分“加强问责制”了解滥用定义。）
123.	RDS 必须建立审核机制来检测隐私/代理服务提供商和安全凭证授权方的滥用情况；例如：建立用于检测不同寻常的行为模式的机制。（请参阅第 VI 部分“改善注册人隐私”了解滥用定义。）
124.	RDS USD 必须在使用条款 (ToU) 中同意审核数据访问，使用和提供准确的身份和目的信息。
125.	RDS 必须制定一个流程，以在未正确验证、存储和保护数据时采取补救措施，对验证方停职或解约。（请参阅第 V 部分“提高数据质量”了解 VR 要求。）
126.	RDS 必须制定一个流程，以在审查不恰当或不充分时采取补救措施，对安全凭证批准方停职或解约。（请参阅第 VII 部分“改善注册人隐私”了解相关要求。）
127.	RDS 必须制定一个流程，以在未正确委任、存储和保护 USD 时采取补救措施，对 RDS 用户委任方停职或解约。（请参阅第 IV 部分“加强问责制”了解 RDS 用户委任方要求。）
128.	ICANN 必须制定 ToS 政策以确保注册管理机构、注册服务商和验证方向 RDS 提供准确、已更新和及时的数据。（请参阅第 VI 部分“法律和合同注意事项”了解将反映在 RIA 和 RAA 中的 RDS 和注册管理机构要求。）
129.	RDS 必须为注册管理机构、注册服务商和验证方制定一个审核流程，并制定一个流程以便在注册管理机构/注册服务商/验证方未提供准确、已更新和及时的数据时向 ICANN 报告。（请参阅第 VI 部分“法律和合同注意事项”了解将反映在 RIA 和 RAA 中的 RDS 和注册管理机构要求。）
130.	RDS 必须建立一个审核机制以持续确保 RDS 收集以及托管提供商存储的数据的质量和完整性。（请参阅第 VIII 部分“数据存储、托管和记录”。）
131.	ICANN 必须建立审核机制来检测 RDS 提供商违反任何 ToC 的情况。例如：允许未授权使用数据、不回复有关数据滥用的投诉、滥用凭证或滥

编号	问责制和审核原则
	用验证。（请参阅第 VI 部分“法律和合同注意事项”。）
132.	ICANN 必须制定一个流程，以在 RDS 提供商未履行合同责任时采取补救措施，对 RDS 提供商停职或解约。例如：可用性、可靠性、隐私、访问权限和性能要求。（请参阅第 VI 部分“法律和合同注意事项”。）
133.	ICANN 必须确定为实现 RDS 的以下主要目标所做的年度改进措施并制定相关基准：(I) 提高数据质量，(ii) 加强问责制，(iii) 改进隐私保护。RDS 必须证实所有三个领域以相似的速度取得了持续的进展，并制定一个流程来确定和解决导致任何领域的改进速度比其他领域更慢的无法预料的问题。

下表汇总了 RDS 生态系统实体与应该对它们应用的问责制和审核要求类型（原则 #114 将做进一步阐述）。

适用的要求	RDS 寻找数据的用户	注册人	注册服务商	注册管理机构	RDS 提供商	ICANN	隐私/代理服务提供商	安全凭证批准方	验证方	RDS 用户委任方	基于目的的联系人	托管提供商
提供准确/可靠的数据		✔	✔	✔	✔		✔	✔	✔		✔	✔
用于指定目的	✔		✔	✔	✔	✔	✔	✔	✔			✔
确保信息安全			✔	✔	✔	✔	✔	✔	✔			✔
验证/鉴定					✔				✔	✔		
及时更新		✔	✔	✔			✔	✔	✔		✔	
执行隐私政策			✔	✔	✔	✔	✔	✔	✔			✔
检测滥用					✔	✔				✔		
投诉流程			✔	✔	✔	✔	✔	✔	✔	✔		
阻止第三方收集				✔	✔				✔			
审核和修正					✔	✔				✔		

表 6：RDS 生态系统实体合规性要求

VII. 改善注册人隐私

EWG 职权范围的核心是如何设置一个系统来提高所收集数据的准确性，同时还要为希望保障和维护其隐私的注册人提供保护。EWG 认识到，个人信息受数据保护法的保护，而且即使没有这类法律，个人也有正当理由寻求对自己个人信息的严格保护。此外，出于某些正当理由，例如在准备启动新的生产线或联系信息会披露个人数据（对小型企业而言）时，一些企业和组织可能会寻求保护它们的信息。

因此，EWG 建议了以下基本原则：

编号	隐私原则
134.	除了通过遵守数据保护法获得隐私权以外，RDS 生态系统还必须满足隐私保护需求，方法是包括以下内容： • 委任的隐私/代理服务，以对通用个人数据进行保护并遵守本地隐私法律；和 • 委任的安全保护凭证服务，为面临风险的个人以及在自由言论权被否决或发言人遭到迫害时提供。
135.	必须对隐私/代理服务提供商进行委任并针对提供和使用委任的隐私/代理服务制定相应的规则。
136.	除了通过委任的隐私/代理服务注册的域名以外，所有注册人必须对他们所注册的域名承担责任。
137.	ICANN 必须调查制定全方位监管 RDS 活动的单一、统一隐私政策（如下所述）的可能性。

除了数据保护法外，其他国家隐私法律和宪法也会保护亿万互联网用户的在线发言和表达其看法的权利，而避免通过他们的观点轻松并且立即追查到其姓名和地址。这些隐私法律包括联合国人权宣言（第 19 条）[28]，该宣言保护表达自由和言论自由的权利，并保护群体、组织、个人和公司（如，媒体和新闻公司）的以下能力甚至是义务：评论、批评和评价领导层的做法、领导层的活动及其对国家/地区、文化或社会的管理。

保护言论自由和表达自由的隐私法律通常确认：需要根据将组织和群体的名称和地址与它们发表的言论分离开来的规定行使这些权利，并且这对于政府、社会、机构群体或社区来说可能非常重要。它们可能会鼓励思想市场，并将开放社会进行交流的需求置于迫害发言人的权力或只是因为某人不喜欢某消息的支持者而预先审判该消息的可能性之上。

隐私法律和宪法权利还会保护结社自由、宗教自由、种族、道德和机构群体。总的来说，它们可能会规定个人或组织在表述不受欢迎或少数派观点时不必公布其姓名/名称或者甚至是地址，以避免他们立即被追查到、被毁谤或是出现更糟糕的情况。在针对任何反对观点的基层政治动荡和对抗的这十年中，隐私法律保护了少数派观点，并使得在线发言人能够强烈要求改变和变革。

这整份报告认识到，在我们谈到隐私和个人信息保护时，我们旨在确认这两组不同的权利；这些权利通常通过不同的立法来加以保护，并且全球的做法也截然不同。

a. 委任的隐私和代理服务原则

当前，提供了一些服务来掩盖使用域名的实体的身份和/或地址。提供这些服务是基于 WHOIS 的开放性本质。虽然存在有许多变体，但《2013 年注册服务商委任协议》定义以下两项服务：

- “隐私服务”，注册域名的受益人通过该服务注册域名而作为注册域名持有者，但 P/P 提供商会为其提供备用的可靠联系信息，以便在注册数据服务 (WHOIS) 或同等服务中显示注册域名持有者的联系信息。
- “代理服务”，注册域名持有者通过该服务许可 P/P 客户使用某注册域名，以向 P/P 客户提供该域名的使用权，注册域名持有者的联系信息将在注册数据服务 (WHOIS) 或同等服务中显示，而不显示 P/P 客户的联系信息。

在这些定义中，“P/P 提供商”或“服务提供商”指隐私/代理服务的提供商，包括注册服务商及其附属机构（如果适用）。“P/P 客户”是指（无论 P/P 提供商使用什么术语）隐私服务和代理服务的被许可人、客户、受益人、受惠方或其他接收者。

当前的隐私或代理服务并不合乎标准；虽然提供商与 ICANN 之间没有合同关系，但 2013 RAA 引入了 ICANN 进行委任的概念及一些基准义务（在“临时规范”中有所反映）。但是，一些提供商也是注册服务商。所有注册服务商均应遵守 RAA，关于代理注册的域名，RAA 规定：[29]

> 3.7.7.3 任何注册域名持有者即便打算向第三方授予域名的使用许可，也仍是该记录的注册域名持有者，须负责提供自身的全面联系信息并负责提供和更新准确的技术和管理联系人详细信息，以便及时解决与注册域名有关的*任何问题*[30]。根据本条款许可第三方使用注册域名的注册域名持有者须对因不当使用注册域名造成的损害承担责任，除非该注册域名持有者在七 (7) 天内将被许可人提供的当前联系人信息和被许可人的身份披露给向注册域名持有者提供可控诉损害合理证据的一方。

当前，代理服务为某个域名注册的 WHOIS 类似于：

域名：EXAMPLE-DOMAIN.COM
创建日期：2011 年 10 月 31 日
到期日期：2013 年 10 月 31 日
上次更新日期：2012 年 9 月 19 日

注册人：
Domains By Proxy, LLC ← 注册人姓名 = 代理
DomainsByProxy.com ← 注册人组织 = 代理
14747 N Northsight Blvd Suite 111, PMB 309 ← 注册人地址 = 代理的地址
Scottsdale, Arizona 85260
United States

管理联系人：[与技术联系人相同]
私有，注册
example-domain.com @domainsbyproxy.com ← 电子邮件 = domain@proxy
Domains By Proxy, LLC ← 名称 = 代理
DomainsByProxy.com ← 组织 = 代理
14747 N Northsight Blvd Suite 111, PMB 309 ← 地址 = 代理的地址
Scottsdale, Arizona 85260
United States
(480) 624-2599 传真 -- (480) 624-2598 ← 电话/传真 = 代理的电话/传真

当前，使用所谓的隐私服务为某个域名注册的 WHOIS 大致类似，但注册人姓名（通常为管理/技术联系人姓名）会直接识别隐私服务客户而不是代理服务提供商的身份。

[29] ICANN 理事会于 2013 年 6 月 27 日批准了新的 2013 RAA；与 2009 RAA 相比，除了增加了 7 天的时间期限外，第 3.7.7.3 节（如此处所述）的内容大致未变。

[30] 注：EWG 建议 ICANN 考虑“任何问题”是否过于宽泛。

今天的隐私和代理服务提供商均未采用任何标准的流程。但是，一些共同的需求在一定程度上得到了满足：

- 将通信传达给当前的隐私或代理服务客户 — 通常由发送至管理/技术联系人的电子邮件地址的自动转发电子邮件完成。许多（但不是所有）提供商提供了传达服务。
- 披露被许可人的身份和代理客户的直接联系详细信息以响应有关域名的投诉。流程、证明文件、响应度和采取的行动各不相同，通常取决于请求者与提供商之间已建立的关系。
- 曝光被许可人的身份，在 WHOIS 中公开代理服务客户的姓名和详细联系信息。
- 如果请求者无法联系到代理服务客户，也无法从代理服务提供商那里得到解决办法，则他们通常会求助于注册服务商（后者可能或不可能隶属于代理服务提供商）。

当前隐私和代理服务中的缺陷都有据可查。[31] 为满足域名注册人和利益主体对于更加统一且可靠的隐私和代理服务（可加强问责制）的需求，EWG 建议了以下原则：

编号	委任的隐私/代理服务原则
	常规
138.	ICANN 必须委任隐私和代理服务提供商[32]。
139.	至少，委任计划必须根据 2013 RAA 规范继续履行隐私/代理承诺。
	委任的隐私服务原则
140.	实体和自然人可以使用未披露注册人详细联系信息的受委任隐私服务注册域名，特定情况（例如，违反服务条款、传唤）除外。
141.	ICANN 必须要求在服务条款中包括特定条款。服务条款中必须包括要求服务提供商在快速除名时设法提供通知的规定。
142.	委任的隐私服务必须（使用通过验证方创建的 PBC）向注册服务商提供所有必需的、基于目的的、准确且可靠的联系人详细联系信息，以联系隐私

[31] 请参阅附录 B 获取记录 WHOIS 以及隐私/代理服务缺陷的研究和报告。

[32] GNSO 已组建了一个工作组来制定隐私/代理服务委任政策。EWG 建议 RDS 重复利用 PPSAI 工作组完成的任何基础性工作，并根据需要进行修改以反映 RDS 访问方法和数据元素 — 最主要的是 P/P 公布的基于目的的联系人。

编号	委任的隐私/代理服务原则
	服务提供商和获得授权代表注册人解决技术、管理和其他问题的实体。
143.	委任的隐私服务必须负责将注册人的转发电子邮件地址中收到的电子邮件传达给注册人。
	委任的代理服务原则
144.	实体和自然人可以使用代表代理服务客户进行域名注册的受委任代理服务来注册域名。
145.	委任的代理服务提供商必须（使用通过验证方创建的 PBC）向注册服务商提供他们自己的注册人姓名和详细联系信息，包括唯一的转发电子邮件地址，以联系获得授权代表代理服务客户注册域名的实体。
146.	作为注册域名持有者，委任的代理服务提供商必须对该域名承担所有常见的注册人责任，包括提供准确且可靠的、必需的基于目的的联系人和其他注册数据。
147.	委任的代理服务必须（使用通过验证方创建的 PBC）向注册服务商提供所有必需的、基于目的的、准确且可靠的联系人详细联系信息，以联系代理服务提供商和获得授权代表代理服务客户解决技术、管理和其他问题的实体。
148.	委任的代理服务必须负责传达注册人的转发电子邮件地址中收到的电子邮件（详细说明请参阅附录 H）。
149.	委任的代理服务必须负责及时响应披露请求（如附录 H 中的上报程序所述）。

b. 安全保护凭证原则

各方确认，对于某些希望在互联网上保持匿名或希望至少避免向那些可能威胁他们的人公开其地址和个人信息的个人和群体，他们有要求加强隐私保护的合法需求。这些当事人可以根据隐私法律（如果存在）行使他们的权利，或使用隐私注册服务。但遗憾的是，对那些真正受到威胁的人而言，这些机制可能还不够安全。如果在互联网上找不到注册人的详细信息，则这些个人或群体的追随者可能会使用社会工程技术向验证方、注册服务商或注册管理机构提出信息请求（由于缺乏设备，这些当事人无法检测到此类请求）。

提供安全保护凭证的目的是为受到威胁的个人和群体提供安全的匿名注册。这可能包括那些希望行使言论自由权利的个人（普遍认为这些人已受到保护），或其身份可能会威胁自身或其家人生命安全的发言人。

下面提供了五个不同的示例：

1. 宗教少数群体

许多管辖区中都存在宗教少数群体，他们受到人口较多的群体的威胁，或由于其自身信仰要素而受到威胁。他们大概希望能够有一个可以向其成员提供信息的网站，但希望对运营网站的地点和方式保守秘密。例如，由于经常遭到炸弹威胁，罗马的犹太教会堂并不披露其地址，但会向知道该地址的成员公布服务时间。

2. 家庭暴力

许多管辖区都为遭受家庭暴力或逃离其攻击者的个人提供某种形式的身份转变。这同样适用于那些逃离某些宗教群体和教派以及那些受证人保护计划保护的个人。遭受家庭暴力的妇女的避难所可能需要在互联网上做广告来宣传其服务，并保障联系地点和指示的安全以便真正的受害者到达该机构，等等。已经转变身份的个人和家庭可能具有建立网站但不披露其真正地址和身份的合法诉求。应该指出的是，许多为政府工作、由于各种原因（通常与国家安全和执法部门相关）改变了身份的个人也需要在工作现场以及私人生活中加强保护。

3. 政治演讲

在世界上的一些国家/地区，反对党或落选的候选人可能会在选举后逃离。他们也可能希望运行一个网站，以便在那里提供在他们祖国所发生事件或他们所遭受迫害的详细信息。执政政府可能会追查该网站，记录该网站上出现的滥用情况后，指控叛国罪或其他罪行。这些是非常微妙的情形，因为言论自由权利在国与国之间存在巨大的差异，并且很少能够反驳叛国罪指控。注册域名的权利是 ICANN 及其委任的注册服务商所需关注的最重要的权利。

4. 种族或其他社会团体

种族群体经常受到骚扰和歧视，因此可能希望运行网站来向其成员提供重要信息。例如，他们可能想要办一个网站，以便其成员可以在那里公布骚扰事件，而不必害怕确认身份和报复。其他群体，如男同性恋者、女同性恋者或变性者，可能想要为他们的群体办一个非常普通的信息性网站，但由于他们国家/地区严格的法律或者治安维持者或仇恨组织的报复，因而害怕暴露成员的身份。为妇女提供健康和营养信息、生育权等信息的站点运营者甚至也存在遭到报复的情况。

5. 在敌对地区工作的新闻记者

在敌对地区报道新闻事件的新闻记者可能需要或想要办一个网站，同时保护他们（包括其合作者、翻译等）的身份和地址信息的安全和隐私。

探讨安全凭证技术

市场上有各种安全凭证，如 Microsoft 的 U-Prove (http://research.microsoft.com/en-us/projects/u-prove/) 和 IBM 的 Identity Mixer (http://researcher.watson.ibm.com/researcher/view_project.php?id=664)。这些方法允许接收者证实各种属性 — 例如，他或她已受某可信机构认可并通过身份验证，他们已为某项权利或服务付费 — 而无需披露有关他们自己的任何个人信息，或提供启用这些属性的交易的任何追查线索。依赖方具有安全的加密证明，对此接收安全凭证的实体具有可信机构的批准，而无需知道他们的身份或他们如何获得该批准。

此类技术可用于建立一个流程，上述面临风险的实体可通过该流程获取已使用安全保护凭证注册的域名。除了负责处理 DNS 问题的必要联系人外，注册服务商和验证方均不了解有关面临风险的实体的身份信息。因此，他们无法以合法方式响应个人或地址信息请求。很明显，人们对技术合规性、滥用和降低这些风险（如下所述）存有顾虑。关键是，对于使用安全凭证注册的域名，注册服务商和注册管理机构将不再承担向易受攻击的个人的攻击者确认这些个人的身份的风险和责任。

运营问题

为了解决与此类服务相关的问题并消除风险，EWG 探讨了以下潜在的情形：

1. 出于所表述的合法目的（商标滥用指控、希望购买或销售域名、希望调查产品安全性等），信息请求者希望确定上述示例 2、3 和 4 中所述个人的真实姓名或地址。请注意，在性命攸关的情况下，注册服务商会很难确定请求者的行为是否具有欺骗性，而且工作人员也无法预料人们可能面临哪些未知威胁，在身份转变的情况下尤其如此。

2. 请求者联系某域名的注册服务商（或指定 PBC 的验证方），就某种犯罪或诽谤活动提出指控，并要求对使用该域名的网站除名。在这些情况下，将遵循注册服务商和代理服务提供商的服务条款，而这可能导致披露请求获取域名被许可人的身份和地址。但是，对于使用安全凭证注册的域名，成功的披露只会导致公布批准安全凭证的可信机构。此时，该可信机构将负责调查潜在的 DNS 滥用。在某些情况下（如，犯罪活动），可能会授权对这些网站进行快速除名。

3. 如果政府机关对政治演讲提出指控，将其提高到叛国罪或其他刑事事件的程度，注册服务商还是可能会被迫对使用通过安全凭证注册的域名的网站应用快速除名，具体取决于管辖区内的相关法律。

即使存在这些限制，安全凭证仍然可以为面临风险的实体提供比当前更高的安全性；如果新 RDS 要求提高数据准确性并加强问责制，则必须提供这样的服务。为完成这一任务，需要开发以下关键功能：

1. 一个流程，用于为面临风险的实体是否有资格使用安全凭证制定标准，从上述用户示例和 ICANN 机构群体认为适合为其制定政策的任何其他实体开始。
2. 申请表、必需的证明文件和财务系统，所有这些项目旨在确保为面临风险的实体（在某些情况下还包括其证明人）的身份提供保护。在任何匿名系统中，这是主要的缺陷之一。
3. 一个独立审核委员会，旨在评估和批准安全凭证申请以及可信方（如，具有授权名称更改的政府、保护难民的联合国组织、国际记者协会等）的证明文件。
4. 可信方（如上述第 3 条所述），这些相关方愿意与该独立审核委员会来回传达安全凭证申请和生成的域名。这些可信方（以下称为“安全凭证接收者”）必须证实面临风险的实体的匿名性需求，并接受安全凭证注册的域名的任何潜在 DNS 滥用的问责。
5. 委任的代理服务提供商，该提供商愿意在注册将由安全凭证批准方授权的域名时接受安全凭证以及他们将通过其付款的财务系统。
6. 有关快速除名程序和其他减少 DNS 滥用情况的政策。这可能包括加强对安全凭证注册域名的安全性监控、阻止潜在的 DNS 误用和滥用，以及帮助防止域名受到攻击。受 DNS 滥用指控的相关方应将他们的案例提交到批准面临风险的实体的申请的委员会；该安全凭证批准方将评估受指控的滥用情况。

下图演示了这些相关方之间可能存在的关系、它们的责任以及它们之间的通信流程。

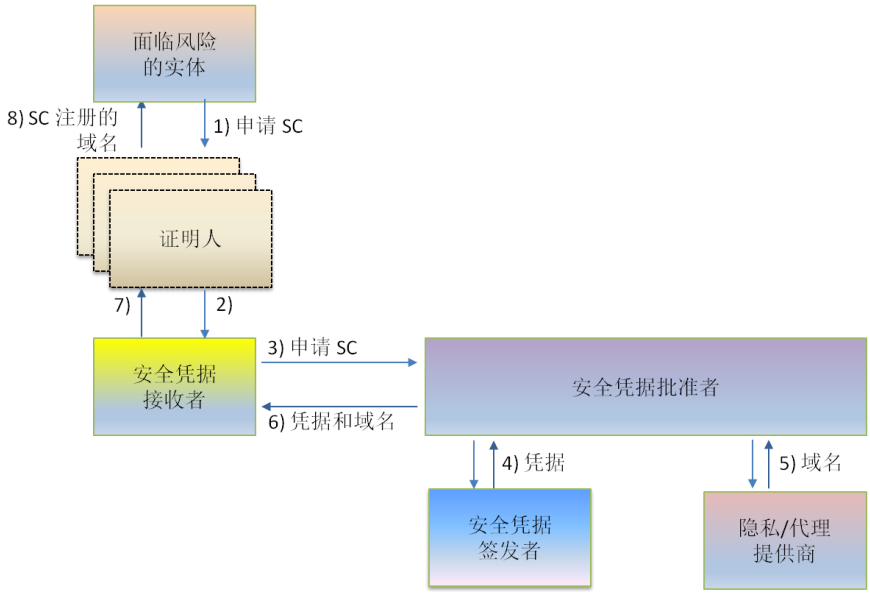


图 8：安全保护凭证模型

剩余风险

安全凭证并未得到广泛采用，因为除了其他原因以外，它们实施起来非常复杂，特别是在注册和撤销方面。人们认为所有相关方应有资格进行此类注册，但考虑到创建此服务并确保不将其用于欺诈或犯罪目的需要做大量工作，EWG 认为该方法并不可行。EWG 建议，应开发安全保护凭证以用于有限用途，并确保自身可以应用该服务的实体确实具有保持匿名的合法要求。

此外，各方还认识到，一旦注册了此类域名并且使用该域名的网站开始运营，各种互联网流量元数据和内容可能会导致确定域名用户的身份。这超出了 ICANN 的职权范围，该机构仅侧重于处理域名注册问题以及为实现 ICANN 职权范围内定义的目的而收集、使用和披露的相关数据。实际使用域名而生成的信息必须由申请并使用安全凭证注册域名的实体负责，并且可能必须提供强调这种风险的信息。ICANN 的职责仅限于域名系统本身。

编号	安全保护凭证原则
150.	能够证实如果被确认身份将会面临风险的个人和群体必须可以匿名申请并接收使用安全凭证注册的域名 — 证明人和可信第三方将帮助在面临风险的实体与注册服务商/验证方之间提供保护。
151.	ICANN 支持建立一个独立可信审核委员会，后者将核实面临风险的组织或个人的声明来批准（并在必要时撤销）凭证。此类组织 — 本文中称为安全凭证批准方 (SCA)— 可以开发其他服务，如对用户进行有关风险和安全互联网实践的培训。
152.	ICANN 必须帮助培养或授权安全凭证签发者，后者将确认批准 SCA 并生成对应的安全凭证。
153.	安全凭证批准方必须使用签发的安全凭证以常规方式通过委任的代理服务提供商授权域名。代理服务提供商的信息将在 RDS 中显示。RDS 将不具有任何有关使用安全凭证注册域名的面临风险的实体的数据，并且必须使用某种匿名或代理付款系统。
154.	使用安全保护凭证注册的域名必须遵循委任的隐私/代理服务提供商的常规披露和除名程序。隐私/代理客户（如，安全凭证批准方）未能及时做出响应或出现滥用 DNS 的证据可能会导致安全凭证注册的域名被快速除名。
155.	认识到使用安全保护凭证注册的域名可能会面临网络攻击的风险，或调查违规行为可能较为困难，认为加强对这些域名的安全性监控可以降低风险。
156.	必须为申请和撤销安全保护凭证制定政策和流程。 • 批准流程必须允许零个或多个证明人为面临风险的实体的身份和位置提供充分保护，以免向 SCA 提交申请的可信安全凭证接收者获知。证明人的人数和身份对 RDS 透明；唯一与 SCA 直接接触的一方是安全凭证接收者。 • 撤销流程必须允许面临风险的个人的身份和位置获得类似保护，同时强制执行安全凭证服务条款。SCA 必须负责调查有关安全凭证的被控 DNS 滥用以及强制执行服务条款。如果 DNS 滥用足够严重，导致需要撤销凭证，SCA 应对安全凭证接收者负责。

c. 隐私性主要优势汇总

提高准确性并加强问责制后，保护个体公民特别是易受攻击的公民将变得更加重要。将数据保护、委任的隐私/代理和安全保护凭证原则与机制作为不可或缺的一部分合并到下一代 RDS 中将强化注册人和联系人的隐私权。

EWG 建议的数据保护原则将：

- 通过应用单一且统一的 RDS 政策、在整个 RDS 生态系统内一致地实施该政策并使用“规则引擎”来应用当地法律，为个人数据提供更一致的保护。
- 需要公布及匿名提供更少的注册和联系数据。
- 为注册人和联系数据提供更强大的保护以防止滥用。

EWG 为委任的隐私/代理服务提供商建议的原则将：

- 通过为提供隐私/代理服务的提供商建立一个委任框架，为寻求此类服务的注册人提供更清晰的描述。
- 要求将域名标识为已使用委任的隐私/代理服务提供商提供的服务进行注册。
- 在注册数据中清楚指明如何联系该隐私/代理服务提供商。
- 阻止第三方未经授权使用委任的隐私/代理服务提供商的联系数据。
- 要求委任的隐私/代理服务提供商将电子邮件传达给基本注册人并响应咨询。
- 向执法部门和其他第三方滥用报告者及披露请求者提供更加一致且可预测的预期。

EWG 建议的安全保护凭证原则将：

- 第一次建立相关程序，以便易受攻击的弱势群体可以获得将他们自己的域名保存在互联网上的各种好处。
- 为那些迫切需要通过互联网获得言论自由以及在群体之间进行交流的个人提供保护，同时对潜在的滥用采取补救措施。
- 解除验证方和注册服务商可能承担的责任，当前，这二者对通过社会工程攻击披露高度敏感的个人信息负有责任。
- 为使用安全保护凭证注册的域名提供额外的安全性。
- 要求对滥用 DNS 的安全保护凭证注册网站予以快速除名。

VIII. 可能的 RDS 模型

a. 模型设计原则

本报告提供了 EWG 探讨的几个备选模型的相关详细信息，并对这些模型可能会如何满足 EWG 建议的原则进行了分析。所有模型均使用如附录 F 中所述的一组多角度标准进行了评估。

在进行分析的过程中，EWG 应用了以下设计原则：

编号	模型设计原则
157.	**收集：**目前，注册服务商或注册服务商的附属机构从它们自己的客户（注册人）那里收集并存储注册信息。本质上，这是一个分布式流程。除了注册服务商或附属机构继续从注册人那里收集注册数据以外，EWG 还建议验证方收集联系数据。
158.	**存储：**有多个可能的模型可用于存储所有 gTLD 中的注册信息。EWG 确定了几个可能的模型，指出了两个似乎最具潜力的模型，并通过应用附录 F **中所述的评估标准选择了一个建议的模型。**
159.	**访问：**为保护数据主体的隐私，必须提供一个集中化接口以便相应的请求者访问所有 gTLD 中的注册信息，包括任何人未经身份验证访问公共数据以及委任用户通过身份验证后访问网关数据。
160.	**协议：**RDS 必须将 RDAP[33] 或 EPP（根据每个接口酌情选择）用作底层目录访问协议，以便从存储位置获取注册信息（无论它位于什么位置）。

b. 考量的模型

为了测试 EWG 在其初步报告中考量的备选系统模型以及 ICANN 机构群体建议的其他模型，EWG 首先确定了应深入分析的模型。每个模型在许多方面（包括如何通过 RDS 复制或查询注册数据）都存在巨大的差异。下表[34]汇总了这些差异，附录 F 提供了详细说明。

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

[34] 模型要点概述表：RR 指注册服务商，Ry 指注册管理机构，V 指验证方

可能的模型	收集	存储	复制	访问
当前 WHOIS	RR	RR/Ry	不适用	RR/Ry
联合	RR 和 V	RR/Ry 和 V	不适用	RDS
同步*	RR 和 V	RR/Ry 和 V	RDS	RDS
地区	RR 和 V	RR/Ry 和 V	地区	RDS
选择退出式	RR 和 V	RR/Ry 和 V	可选	RDS
旁路	RR 和 V	RR 和 V	RDS	RDS

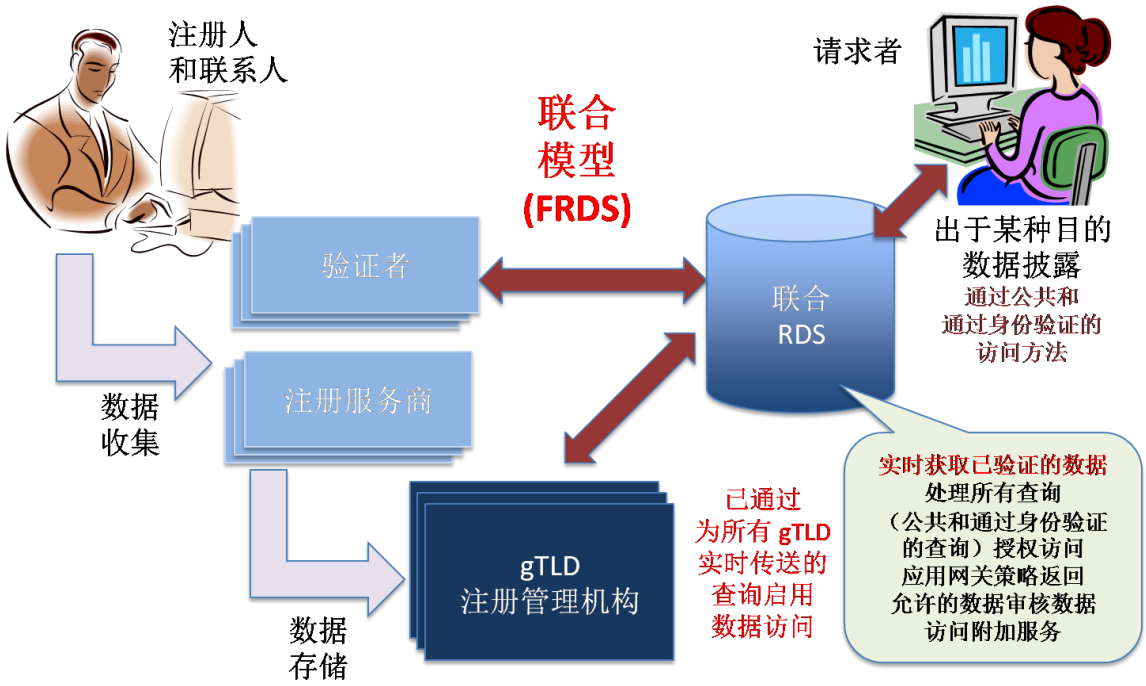
*** 注：**此模型以前称为**“集中式 RDS (ARDS)”**，现在重命名为**“同步 RDS (SRDS)”**，以更好地反映该模型按照一致、协调的方式使用位于多个位置的数据的特性。此处考量的所有模型将使用工程最佳实践部署以实现容错、高可用性和负载均衡，这些实践包括分布于不同地域的数据中心、稳定而多样的连接，以及每个数据中心的冗余基础架构。

c. 建议的模型

上述可能的系统模型在通过 RDS 复制或查询注册信息方面各有差异。EWG 仔细分析了每一个模型，以确定这些差异对各种属性的可能影响。在比较这些可能的模型后，EWG 发现除了当前的 WHOIS 以外，所有模型都能够在一定程度上满足 EWG 建议的 RDS 原则。其中，EWG 重点对以下两个最具潜力的模型做进一步考察：联合模型和同步模型（以前称为“集中式模型”），**并最终建议采用同步模型 (SRDS)。**

联合模型（第二名）

此模型介绍了这样一个 RDS：它从由详细注册管理机构和验证方（这二者全都使用常用的联合数据架构）运营的分布式存储区域提取注册信息。没有任何数据集中到单一存储位置，而是统一通过该 RDS 公开/网关访问从所有 gTLD 注册管理机构（域名数据）和验证方（联系人详细信息）处实时获取的注册信息。



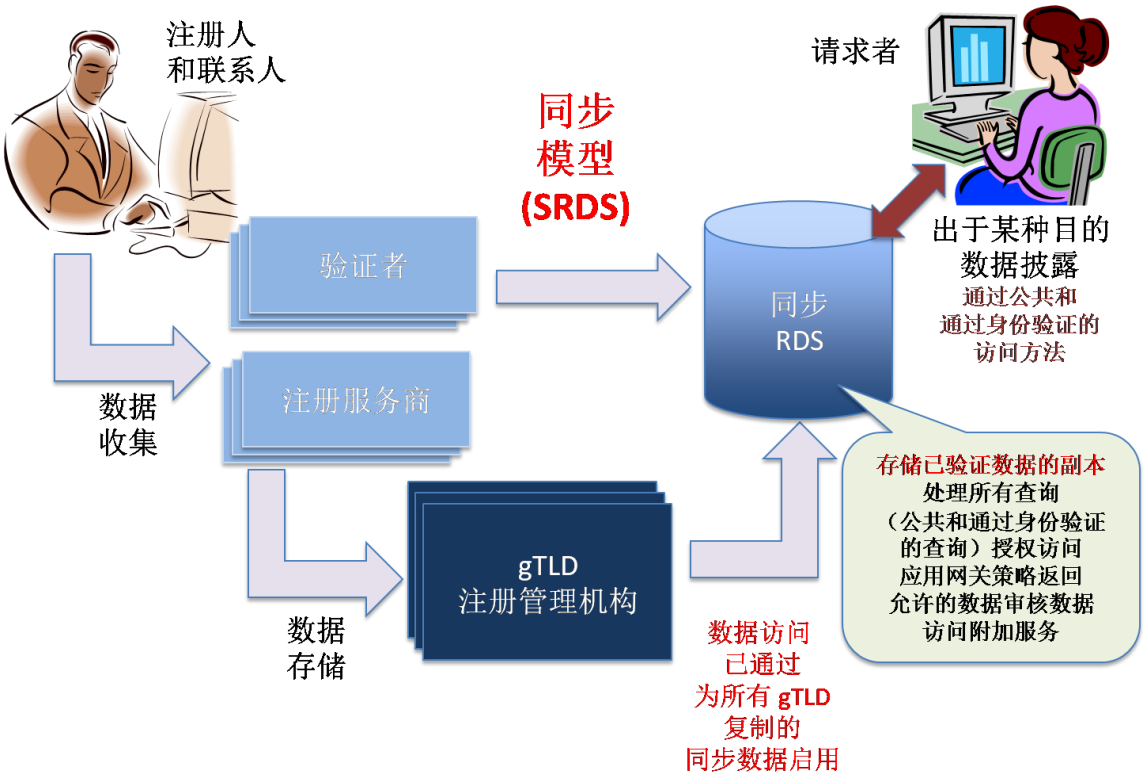
在此模型中，FRDS 将通过 RDAP 从验证方和注册服务商/注册管理机构处提取数据。附录 I（RDS 流程图）进一步详细说明了与此模型相关的联系人和注册数据流，附录 E 使用示例查询进行了演示。

同步模型 (SRDS)（建议采用）

此模型介绍了这样一个 RDS：它几乎实时地将详细注册管理机构和验证方共同负责运营的分布式存储区域收到的数据复制到一个同步系统中，后者将集中这些数据并将其存储到该 RDS 运营的分布式体系架构中。

如前所述，在此模型下，该 RDS 将作为权威数据源并提供权威访问。因此，该 RDS 将超出为注册服务商和注册管理机构及时进行更新制定的当前 RAA 要求（以及当前需求）。注册管理机构、注册服务商和验证方可以向客户提供访问他们自己数据的权限，但所有网关数据请求必须通过查询该 RDS 来做出响应。此模型旨在响应以前的 WHOIS 建议和以下请求：减少消费者对于在什么地方以及如何访问注册数据的困惑，同时最大限度地降低注册服务商和注册管理机构的成本并减少问责制要求。

虽然该 RDS 提供了数据访问权限，但数据不是存储在单一位置，而是存储在多个位置，这些位置针对需要容错、高可用性和负载均衡的系统根据工程最佳实践进行了多样化和冗余处理。注册管理机构和验证方将继续存储它们自己的数据，但该 RDS 可使用数据的同步副本更高效地处理访问请求。



在此模型中，数据将通过 EPP 由验证方和注册服务商/注册管理机构推送到 SRDS。附录 I（RDS 流程图）进一步详细说明了与此模型相关的联系人和注册数据流，附录 E 使用示例查询进行了演示。在应用附录 F 中介绍的方法之后，下文将对 EWG 首选的这两个模型进行相对比较。

- **安全性影响** – 在对它们的安全性影响进行评估时，这两个模型生成了类似的结果。虽然有公众意见认为集中式（随后重命名为“同步”）模型（例如，初步报告中建议的模型）由于集中式接口中的“单一故障点”会造成风险，但 EWG 发现，该风险与大型 gTLD 注册管理机构和全球规模的互联网网站当前构成的风险并无不同。当前的最佳实践表明，基于信息的大型系统会利用多个数据中心、备份存储和灾难恢复系统，以及分布于不同地域且完全冗余的基础架构来降低这些风险。

同步模型具有能够确保一致地实施安全功能以及执行政策的附加优势。通过严格操作系统组件，与联合模型相比，采用由某个运营商管理的分布式体系结构的同步模型可能会生成更加统一的方法来实现预定的安全性目标。在某种程度上，这是因为在联合模型中，可能有数千个注册管理机构、注册服务商和验证方管理着它们各自的数据库，而且注册管理机构/注册服务商/验证方的专业技能水平以及在安全实践方面的投资也各不相同。

- **管辖区和隐私问题** — 在评估管辖区和隐私权影响时，这两个模型生成了类似的结果。在联合模型中，数据在注册管理机构级别进行存储和控制，附加副本保存在其他位置（即，注册服务商、验证方的位置，以及全球各地的备份数据中心）。同步模型则在多个与注册管理机构分离的位置存储和控制数据，附加副本保存在其他位置（注册服务商、注册管理机构、验证方和全球各地的备份数据中心）。分析评估的所有模型后发现，大多数模型都无法避免将数据传输到多个位置，但“旁路模型”除外，该模型不需要注册管理机构存储联系数据。

  此外，同步模型支持以更加一致的方式应用相关规则来满足当地隐私要求，因为管理由一个实体（同步 RDS 的运营商）管理的规则会更加容易，而在联合模型中可能有数千个参与者进行管理。

- **委任** — 同步模型和联合模型都可能会应用委任要求。虽然这两个模型都可以提供相关功能来跟踪和制约委任系统的滥用者，但在数据库由一个实体管理的同步模型中，这样做会更加方便，而在联合模型中可能存在数千个参与者。此外，实施联合模型需要额外的开支，以及确定详细的合同义务，签订服务水平协议并由 ICANN 进行合规性监管来支持一致的执行和审核功能。

- **操作** — 同步模型提高了一些操作区域的效率，而在联合模型中更难实现这种效率。例如，在同步模型中，由于能够以更加一致的格式翻译或音译联系数据，因此可以更加轻松地部署以多种语言/文字显示数据的界面友好的门户。在联合模型中，要获得类似的一致性，各种协议需要清楚阐明翻译/音译标准规范。虽然可以将这两个模型设计为允许进行随机数据质量审核，但在同步模型中可能更易于完成该任务。

  联合模型中的数据延迟和同步问题有所减少，因为要显示的数据直接来自注册管理机构自身。不过，从同步模型中提取数据会造成延迟问题，但通过要求验证方和注册服务商（通过注册管理机构）及时将 EPP 更新推送到 SRDS（请参阅合规性原则 #108）就可解决这些问题。

- **实施** — 与同步模型相比，联合模型更符合当前 WHOIS 的分布式模型。但是，提供 EWG 建议的强大功能所需的性能要求和搜索能力需要的详细规范和绩效衡量标准都要远超于当前 WHOIS 提供的那些规范和标准。将需要更严格的 ICANN 合规性监管以及更多的资源才能确保联合系统中各方的绩效符合预期。在任何一个模型中，受影响的参与者都需要更新他们的软件平台，以与 RDS 接口交互来提供搜索结果和所需的联系数据。

- **成本** — 使用同步模型可以减轻联合系统中所需的即时响应来自 RDS 接口的复杂查询（如，反向查询）的运营负担，因此注册服务商和注册管理机构（还包括验证方）可以实现一些成本节省。具体来说，模型成本比较（附录 F 中提供了详细说明）得出以下结论：

  (1) 在应用相关假设的情况下，与同步 RDS (SRDS) 模型相比，联合 RDS (FRDS) 模型中核心 RDS 系统的成本要略低一些。但是，联合模型对于反向查询的数量高度敏感。**如果反向查询的数量更大，则与 SRDS 模型相比，FRDS 模型的成本要大得多。**例如，在反向查询负载为 3% 而不是 1% 的情况下，FRDS 模型的成本要比 SRDS 模型的成本高 35%。如果反向查询数量达到 5%，则总体 FRDS 成本预计会增加约 85%。这是与 FRDS 模型相关的一个重要的不确定风险因素。人们认为 SRDS 模型对于反向查询的数量不太敏感。

  (2) 此外，**由于 FRDS 模型对于注册管理执行机构有[更大的成本]影响，因此它在整个生态系统中的成本更高。**在 FRDS 模型中，每个注册管理执行机构必须实时实施和支持（根据 SLA）针对 RDS RDAP 查询的响应，包括反向查询和历史 WhoWas 查询。对于后者，注册管理执行机构还必须维护历史数据，这进一步增加了注册管理机构的成本。请注意，每个注册管理机构的这笔附加成本可能超出了上面估计的核心 RDS 系统影响。

  (3) 此外，与 SRDS 模型相比，**FDRS 模型还需要更高的应用程序操作、支持、维护和测试成本**，因为预计它会与注册管理执行机构进行更多交互。

有关该模型的成本分析、其范围和方法、基本度量标准和假设的更多详细信息，请参阅附录 F 和 IBM 于 2014 年 3 月为 ICANN 准备的“*注册目录服务 (RDS) 实施模型成本分析*[35]”。

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

d. 数据存储、托管和记录原则

编号	存储、托管和记录通用要求
161.	必须制定位置、保留、隐私和访问政策。
162.	存储、托管和记录政策与实施必须遵守本地和国际法律。
	存储原则
163.	为了维护冗余系统和消除单点故障，数据应位于多个位置（如，验证方、注册服务商、注册管理机构、托管提供商和 RDS 提供商）。
164.	存储在多个位置的数据必须保持一致。
165.	RDS 必须保障存在风险的数据元素的安全性、保密性和完整性，防止有人未经授权而披露或使用。
166.	必须无期限地存储交易数据，以维护长期以来数据更改的准确记录并支持 WhoWas 功能，但不能超出遵守可适用的数据保护法所需的限制（如果有）。还应依法定期（例如，取消关联一年后）清除孤立的联系信息。
	托管[36]原则
167.	必须对托管数据进行审核以检查其格式是否正确，寄存是否完整无遗。
168.	与同步 RDS 模型配合使用时可能更易于进行托管和托管审核。
169.	托管数据本身必须进行加密并且对审核机构不透明。
170.	必须根据《注册服务商委任协议》、个体《gTLD 注册管理机构协议》和可适用数据保护法的要求将托管数据保留一段时间。当前，这段时间为发布实体的数据赞助期间加上此后两年或更长时间（如果《gTLD 注册管理机构协议》要求），但不能超出法律允许的最长时间。
	记录原则
171.	必须记录 RDS 查询以提供系统使用方式的记录。
172.	可能需要聚合日志以检测分布式系统指示的滥用情况。
173.	必须记录更改以提供一段时间内的数据元素历史记录。

[36] 托管是指将加密系统备份到可信第三方（托管提供商）以便在灾难、系统故障等情况下进行恢复。请参阅 RAA 了解更多详细信息。

174.	必须将运营 RDS 日志的访问权限定于那些具有特定目的并且“须知”的可信、通过身份验证且获得授权的个人和实体。这必须包括 RDS 授权运营商本身（以确认正确的 RDS 运营并进行故障排除）和授权数据保护实体（以监控 RDS 是否符合数据保护立法）。（另请参阅第 VIII(b) 部分“执法部门访问”。）

IX. 成本和影响

a. 成本原则

如附录 F“模型比较方法”中所述，EWG 还考量了 RDS 成本和影响。EWG 承认，建议模型的某些方面会带来新的成本，但认为目前低效且经常不够准确的 WHOIS 系统产生的许多其他隐性成本将会减少。因为建议的 RDS 会提供改良的新服务，因此必须对成本和利益进行评估。建议的方法将首次为政策制定者提供相关选项，以便为那些从系统中请求注册数据的人想出办法，为该系统的运营做有效的贡献。

目前运营 WHOIS 的成本尚不可知，但包括整个生态系统的成本，而不仅仅是提供 WHOIS 服务的注册管理机构和注册服务商的成本。注册服务商不需要划分 WHOIS 成本，并且可能难以区分为 gTLD 和 ccTLD 提供此类服务的成本。当前 WHOIS 的低效和缺陷会给生态系统内的其他参与者带来成本，例如，商标持有者需要向品牌保护公司支付服务费用以及购买商业 WHOIS 服务来确定域名抢注者。

EWG 建议了以下成本原则：

编号	成本原则
175.	必须可以免费未经身份验证（无网关）访问公共数据。
176.	执法部门经身份验证（网关）访问授权数据元素（根据正当程序）可能应服从特殊的成本考虑要素。
177.	RDS 设计应努力获得成本效益并最大限度地降低成本，而不影响其他目标。
178.	RDS 应以成本回收模式运营。
179.	为便于从 WHOIS 进行迁移，应创建一个 RDS 软件开发平台并由 ICANN 提供资金，以最大限度地降低注册服务商/注册管理机构、验证方和 RDS 用户委任方的 RDS 实施成本。
180.	提供此软件开发平台不应给其他 RDS 用户造成沉重的负担。

如果不深入分析特定实施细节，可以在整个生态系统内分摊成本。可以回收成本的示例包括：根据用户、所访问的数据元素或用途征收各种许可费（如，商业使用费、超级用户的订阅费或高级访问费），或为相关服务收取的费用（如，证书审核费或预验证费）。

RDS 还可以为不再需要提供公共访问或满足严格服务水平响应时间的注册管理机构和注册服务商节省成本。通过减少由于提供商（注册服务商、注册管理机构、验证方或委任的隐私/代理服务提供商）不合规而造成的效率低下现象，希望获取数据的请求者也可以实现成本节省。

b. 根据 2013 RAA 与当前 WHOIS 相比的优势

过去十年来，各种报告和研究已记录了 WHOIS 的缺陷，详见附录 B。新《2013 年注册服务商委任协议 (2013 RAA)》中体现的 WHOIS 改进，以及由于 ICANN 理事会评估 WHOIS 审核小组建议而实现的其他改进已经弥补了在 WHOIS 中发现的一些缺陷。

虽然 2013 RAA 引入了一些新的义务以及引人关注的验证和核实要求来提高准确性，但其他重要缺陷仍然继续存在。下面汇总了这些缺陷（与本报告中包含为实现其他利益而提出的建议的各个部分相对应）。

2013 RAA 中 WHOIS 的缺陷	由 RDS 解决/所在部分
匿名公开访问所有数据元素会创建一个可能发生采集和滥用、缺乏问责制或无法纠正的环境	第 III 部分：用户/目的 第 IV 部分：加强问责制 第 VI(d) 部分：问责制和审核
保护个人隐私的能力有限	第 VI(a) 部分：数据保护 第 VII 部分：改善注册人隐私
确保注册数据完整性的能力有限；注册人可以轻松插入虚假的联系信息，包括那些由他人持有的信息	第 V 部分：提高数据质量 第 V(g) 部分：唯一的联系数据功能
缺乏安全功能	第 IV(b) 部分：未经身份验证和网关数据访问 第 IV(c) 部分：RDS 用户委任
缺乏审核功能	第 VI(d) 部分：问责制和审核 第 VIII(d) 部分：数据存储、托管和记录

2013 RAA 中 WHOIS 的缺陷	由 RDS 解决/所在部分
访问与规定的合法目的没有直接联系	第 III 部分：用户/目的 第 III(e) 部分：基于目的的联系人
WHOIS 查询接口和响应不一致	第 IV(b) 部分：未经身份验证和网关数据访问 第 VIII 部分：可能的 RDS 模型
不支持显示国际化注册数据或无相关标准	第 IV(b) 部分：未经身份验证和网关数据访问 第 V(e) 部分：与验证方交互
应用不同规则以遵照各种数据隐私制度的能力有限	第 VI(a) 部分：数据保护
无法接受的准确程度导致那些希望与注册人通信的相关方效率低下	第 V 部分：提高数据质量 第 III(e) 部分：基于目的的联系人
用于在多个域名间更新联系人的管理流程较为繁琐	第 V 部分：提高数据质量 第 V(c) 部分：准确性、审核和修正流程
难以确定隐私和代理服务客户的身份并与其进行通信	第 III(e) 部分：基于目的的联系人 第 VII(a) 部分：隐私/代理服务 附录 H：传达与披露模型
除了仅适用于注册服务商及其附属机构的 2013 RAA 要求以外，没有其他隐私或代理服务规章	第 VII(a) 部分：隐私/代理服务 附录 H：传达与披露模型

c. 风险和影响评估

如第 IV 部分“加强问责制”所述，EWG 建议执行一次范围广泛的风险评估，以确认本文建议的 RDS 原则确实导致适当收集和披露数据以用于定义的目的，从而在风险与利益之间达成理想的平衡。

3 月 14 日，EWG 邀请提供或使用 gTLD 域名注册数据的所有相关方参与 RDS 风险在线调查；这些相关方包括注册人、注册服务商、注册管理机构，以及当前使用 WHOIS 数据的不同个人、企业和其他组织。此调查使受访者有机会向 EWG 说明下一代 WHOIS 替代系统可能给他们带来的风险和利益。

在本报告定稿前，EWG 分析了通过此调查确定的风险和利益的速览，希望降低无法预期和不必要的风险。截至 2014 年 5 月 29 日，此调查的英语版本已收到 180 份部分回应，其中约 100 份完成了整个调查。到目前为止，受访者分别来自北美 (68%)、欧洲 (35%)、亚洲 (20%)、拉美 (14%)、非洲 (11%) 和大洋洲 (10%)，其中使用和提供注册数据的受访者各占一半。这些回应揭示了以下领域中最可能存在并且影响深远的风险和利益：技术、运营、法律和财务、安全和隐私。约有二十多位受访者还就无法避免但可接受的风险以及转移或降低风险的方式提出了建议。

为便于机构群体就此主题广泛发表意见，EWG 已决定将 RDS 风险调查一直开放到 2014 年 7 月，并且推出翻译版本。调查回应将用于为 ICANN 理事会审查本报告提供参考，并作为向所有将受 RDS 替代 WHOIS 影响的利益主体将来进行正式的成本、风险和利益分析提出的意见[37]。

[37] 另请参阅 ICANN 的 DNS 风险评估（第一次复议）公众意见征询

X. 结论及后续措施

考虑生态系统内依赖注册数据的许多利益主体的观点后，EWG 一致建议废弃授予每个用户相同的匿名公共访问来访问 gTLD 注册数据的当前 WHOIS 模型，而采用一个从零构建的替代系统。

EWG 认为，与目前现有的原则和 RDS 相比，本最终报告中建议的原则和下一代 RDS 将提供一个更加坚实的基础 — 将在此基础上保护个人隐私，确保提高整个 ICANN 生态系统在来年的准确性、问责制和透明度。该 RDS 建立在根据最近协商的 2013 RAA 所做的改进基础之上，但范围远远超出这些改进，第 IX(b) 部分提供了详细说明。

虽然对一些人来说，此最终报告似乎过于详细，但它并不全面。如附录 A 所述，该报告解决了理事会提出的每个问题。但是，一些问题仍有待在将来得到充分解决 — 通过任何后续的政策制定流程 (PDP) 或任何相关实施工作。

- **RDS 用户群体委任机构和政策。**由于特定用户群体可能有权访问网关数据以用于批准的目的，因此，应在实施阶段审查用于确定谁有资格作为该群体成员的政策，以确定可能适合每个群体的委任机构和模型。
- **EPP 和 RDAP 所需的扩展。**如附录 G 所述，EWG 建议使用标准协议来支持 RDS 需求，但已确定需要进行某些扩展来为建议的 RDS 模型和数据元素提供全面支持。
- **风险和影响评估。**如第 IX 部分所述，EWG 建议在实施建议的 RDS 之前进行全面风险评估和成本/利益分析，并已启动了一项调查来收集对该流程的意见。
- **RDS 隐私政策。**如第 VII 部分所述，EWG 建议根据隐私保护的标准最佳实践为 RDS 起草基本的 ICANN 隐私政策，并且制定在整个 RDS 生态系统内实施此政策的标准合同条款。
- **联系数据的翻译/音译。**由于当前正就此问题启动政策制定流程 (PDP)，除了在第 IV(b) 部分中确定的原则外，EWG 选择不做重复性工作，而是建议在将来分析当前 PDP 的结果来确定如何将任何新政策应用于 RDS。
- **隐私和代理服务。**将需要结合 GNSO 中就此主题展开的工作考量 EWG 的与委任的隐私/代理服务提供商相关的建议，使当前 PDP 的结果与实施的任何 RDS 保持一致。
- **验证方生态系统。**需要在实施阶段进一步研究是否为验证方制定委任计划，以及用于验证位于世界各地的注册人和联系人的详细联系信息的流程。

RDS 反映了对无法分割的相互依赖元素所精心作出的均衡折中考虑。EWG 在许多公众意见征询、网络会议中收到的意见以及就其迄今为止开展的工作进行的磋商为这些折中考虑提供了参考。因此，EWG 鼓励理事会将最终报告转发给 GNSO 以便整体采纳。选择采纳部分而不是所有这些 RDS 设计原则会损害整个生态系统的预期利益。EWG 担心，单独分析各个组件可能会导致机构群体重复提出在过去尝试改进 WHOIS 时已经提出的异议并因此陷入僵局。

EWG 已向 ICANN 首席执行官和理事会提交了此最终报告，在线公开发布了该报告，并将在 ICANN 2014 年 6 月的伦敦会议期间召开多个会议。它还将召开网络会议并利用其他机会讨论该报告以及回答 ICANN 机构群体的相关问题。该最终报告将作为理事会为提供 gTLD 注册数据和在适当时进行合同谈判而请求的 GNSO 政策制定流程 (PDP) 的基础。EWG 建议理事会和 ICANN 机构群体在讨论该最终报告时应侧重于以下问题：

- RDS 是否优于当前的 WHOIS 系统？
- 如果否，ICANN 机构群体是否同意继续使用当前的 WHOIS 系统，以及该系统是否能够满足不断发展的全球互联网的要求？

EWG 相信，此最终报告将履行 ICANN 理事会的指令，重新定义 gTLD 注册数据的用途和提供方式，并为帮助 ICANN 机构群体（通过 GNSO）为 gTLD 目录服务制定新的全球政策打下坚实的基础。

附录 A：对理事会问题的回应

为 EWG 的工作提供指导的理事会决议中包括了一系列该工作组要在其进行分析时解答的特定问题。本附录参考了此报告中解决理事会问题的部分。

理事会问题和指导	报告中的对应部分
EWG 将重新定义以下活动的目的： • 收集、 • 维护和 • 提供 gTLD 注册数据的访问权限，以及 • 考虑保护数据的安全措施	第 III 部分：用户和目的 第 VI 部分：加强问责制
为什么收集数据？	第 III 部分：用户和目的 第 VI(a) 部分：数据元素
数据有什么用途？	附录 D：目的和数据需求
谁来收集数据？	第 V 部分：提高数据质量 附录 I：RDS 流程图
数据在哪里存储？存储多久？	第 VIII 部分：可能的 RDS 模型 第 VIII(d) 部分：数据存储
数据在哪里托管？托管多久？	第 VIII(d) 部分：数据存储、托管和记录原则
谁需要数据？原因是什么？	第 III 部分：用户和目的
谁需要访问数据的访问日志？原因是什么？	第 VI(d) 部分：问责制和审核原则
是否可以公开访问有关域名注册的详细信息？	第 IV(b) 部分：未经身份验证和网关数据访问 第 VI(a) 部分：数据元素 第 VII 部分：改善注册人隐私
执法部门是否可以访问有关域名注册的详细信息？	第 III 部分：用户和目的 第 VI(b) 部分：执法部门的数据访问原则
知识产权所有者是否可以访问有关域名注册的详细信息？	第 III 部分：用户和目的
安全专业人员是否可以访问有关域名注册的详细信息？	第 III 部分：用户和目的
公众通过访问注册数据将实现哪些价值？	第 II(b) 部分：目的 第 III 部分：用户和目的
在所有可用的注册数据中，公众需要访问哪些数据？	第 VI(a) 部分：数据元素

理事会问题和指导	报告中的对应部分
WHOIS 协议是否是提供该访问的最佳选择？	第 IV(b) 部分：未经身份验证和网关数据访问 附录 G：EPP 和 RDAP 协议为 RDS 提供支持的能力
安全性	
合法的执法部门需要由哪些部门构成？	第 III 部分：用户和目的 第 VI(b) 部分：执法部门的数据访问原则
如何确定执法人员的身份？	第 IV(c) 部分：RDS 用户委任原则 第 VI(b) 部分：执法部门的数据访问原则
责任方的真实身份由哪些注册数据构成？这些数据的准确程度如何？	第 V 部分：提高数据质量 第 VI(a) 部分：数据元素 第 VII(b) 部分：安全保护凭证
对寻找责任方的真实身份的执法人员而言，哪些注册数据是有价值的信息？这些数据的准确程度如何？	第 III 部分：用户和目的 附录 D：目的和数据需求
WHOIS 协议是否是提供该信息的最佳选择？	第 IV(b) 部分：未经身份验证和网关数据访问 附录 G：EPP 和 RDAP 协议为 RDS 提供支持的能力
知识产权所有者	
所需域名注册数据访问权限是否与其他行业的知识产权所有者访问类似数据具有的权限相一致？	第 III 部分：用户和目的 第 IV(c) 部分：RDS 用户委任原则
如果确定知识产权所有者的身份？	第 IV(c) 部分：RDS 用户委任原则
在所有可用的注册数据中，知识产权所有者需要访问哪些数据？	第 III 部分：用户和目的 附录 D：目的和数据需求
哪些注册数据适合公开？	第 VI(a) 部分：数据元素
WHOIS 协议是否是适合的访问方法？	第 IV(b) 部分：未经身份验证和网关数据访问 附录 G：EPP 和 RDAP 协议为 RDS 提供支持的能力

附录 B：评估 WHOIS 缺陷的研究

- SSAC - SAC 051 报告
- SSAC - SAC 054 报告
- SSAC - SAC 055 报告
- GAC WHOIS 原则
- WHOIS 政策审查小组最终报告
- 处理 WHOIS 与隐私法之间冲突的 ICANN 程序草案
- WHOIS 服务要求清单 — 最终报告
- WHOIS 任务组 2 初步报告 (2009)
- 任务组有关 WHOIS 服务的最终报告 (2007)
- 评估提交和显示国际化联系数据的解决方案的研究
- GNSO 详细 WHOIS 最终报告
- EWG 有关国际化注册数据的中期报告
- 对处理 WHOIS 与隐私法之间冲突的 ICANN 程序进行审核
- GNSO WHOIS 研究，包括
    - WHOIS 注册人联系信息准确性研究
    - 使用排名前 5 的 gTLD 中的隐私或代理服务注册域名的普遍程度研究
    - WHOIS 滥用研究
    - WHOIS 注册人识别研究
    - WHOIS 隐私和代理服务滥用研究
    - WHOIS 代理/隐私披露与传达可行性调查 + 附录

附录 C：使用案例示例

如第 III 部分所述，EWG 分析了涉及当前 WHOIS 系统的实际使用案例，以确定希望访问 gTLD 注册数据的用户、他们这样做的目的以及相关利益主体和数据。EWG 考量的代表性使用案例列表如下所示。

目的	使用案例示例
域名控制	创建域名注册帐户
	域名数据修改监测
	域名投资组合管理
	域名迁移启动
	域名删除
	更新域名 DNS
	域名续用
	域名联系信息验证
个人数据保护	联系隐私/代理服务提供商
	联系安全凭证批准方
解决技术问题	联系域名技术人员
域名认证	签发域名认证
个人互联网使用	联系现实世界
	消费者保护
企业域名的 购买或销售	通过经纪人销售域名
	域名商标通关
	域名收购
	域名购买查询
	域名注册历史记录
	指定注册人注册的域名
学术/公众利益 域名研究	域名注册历史记录
	指定联系人注册的域名
	调查域名注册人或指定联系人
法律诉讼	域名用户联系信息
	打击对注册人数据的欺诈性使用行为
	域名注册人历史记录
	指定联系人注册的域名

目的	使用案例示例
监管和合同的执行	网上税务调查
	UDRP 程序
	RDS 生态系统的合同合规性
犯罪调查和 减少 DNS 滥用	调查遭到滥用的域名
	调查离线犯罪活动
	域名声誉服务
	调查网络犯罪活动
	被攻击域名的滥用问题联系人
DNS 透明度	访问公共注册数据
互联网恶意活动	域名劫持
	恶意注册域名
	挖掘注册数据用于发送垃圾邮件/进行网络诈骗

表 7：使用案例示例

为说明 EWG 所使用的方法，下面提供了一个使用案例。请参阅第 III 部分，了解每个使用案例以及相关 RDS 用户和数据需求的其他说明。

解决技术问题 — 与域名技术人员联系

目标/情景 #1

某人注册的域名出现运营或技术问题。他想知道，他是否可以联系某人以实时或几乎实时地解决该问题，于是他使用 RDS 来确定能够解决问题的适当人员、角色或实体。示例技术问题的不完整列表包括电子邮件发送和交付问题、DNS 解析问题和网站功能问题。

简要格式的使用案例

使用案例：确定可帮助解决域名技术问题的人员、角色或实体。

主要使用案例：某人访问 RDS 来获取与一个或多个 TLD 下的注册域名关联的联系信息。该人员向 RDS 提交一个域名以进行处理。RDS 返回与该域名关联的、确定可与其联系以解决技术问题的人员、角色或实体的信息。

非正式格式的使用案例

标题：确定可解决域名技术问题的人员、角色或实体。

主要参与者：注册域名出现技术问题的人员。

其他利益主体：RDS 运营商；与注册域名关联的可解决技术问题的人员、角色或实体；注册人（该人员可能希望了解运营问题的相关信息）；验证方（该人员可能已为技术联系人签发了联系人 ID）；注册服务商或托管提供商（该提供商可能正提供运营服务）；委任的隐私/代理服务提供商（该提供商可能会帮助联系与域名关联的可解决技术问题的人员、角色或实体）。

范围：与 RDS 交互

级别：用户任务

数据元素：在此使用案例中，允许实时或几乎实时通信的数据元素最为有用。这些元素包括电子邮件地址、即时消息地址、电话号码和/或标识注册人指定的首选联系方式的指示符。RFC 2142 第 4 部分介绍了就 abuse@、noc@ 和 security@ 电子邮件地址提出的建议，这些地址用于“为使用组织的互联网服务遇到困难的客户、提供商和其他人提供援助”，但需要注意的是，由于这些地址属于公共地址，它们往往会吸引大量未经请求的电子邮件发送者。

情况：注册域名出现技术问题的个人（请求者）访问 RDS 以获取一个或多个 TLD 下的注册域名的相关信息。可以通过网站或其他某种电子处理方式访问 RDS。

请求者向系统提交一个域名以进行处理。

RDS 处理该请求，然后报告错误条件，或继续查询 gTLD 注册数据，从而检索之前已标识为可帮助解决此域名技术问题的资源的个人、角色或实体的相关信息。

RDS 返回与该域名或在检索数据时遇到的错误条件关联的注册数据。

图 9：使用案例示例

附录 D：目的和数据需求

EWG 分析了使用案例，以确定希望访问 gTLD 注册数据的用户、他们这样做的目的以及相关利益主体和数据。下表汇总了第 IV 部分中建议的 RDS 数据元素，并将其与第 III 部分中定义的容许目的对应起来。请参阅第 IV 部分，获取每种数据元素的收集和披露建议。

数据元素	目的
域名	所有
DNS 服务器	域名控制 解决技术问题 域名认证 企业域名购买/销售 学术/公众利益 DNS 研究 监管/合同的执行 犯罪调查/减少 DNS 滥用
注册人姓名和/或组织 注册人类型 注册人联系人 ID 注册人联系人验证状态 注册人联系人上次更新时间戳	所有
注册人公司标识符	域名控制 域名认证 个人互联网使用 企业域名购买/销售 法律诉讼 学术/公众利益 DNS 研究 监管/合同的执行 犯罪调查/减少 DNS 滥用 DNS 透明度
注册人邮政地址，包括： 注册人街道地址 注册人所在城市 注册人所在州/省 注册人邮编 注册人所在国家/地区	域名控制 域名认证 企业域名购买/销售* 学术/公众利益 DNS 研究* 法律诉讼* 监管/合同的执行 犯罪调查/减少 DNS 滥用
注册人电话 + 分机 注册人备用电话 + 分机	域名控制 解决技术问题 域名认证 企业域名购买/销售* 学术/公众利益 DNS 研究* 法律诉讼* 监管/合同的执行 犯罪调查/减少 DNS 滥用
注册人电子邮件地址 注册人备用电子邮件	所有

数据元素	目的
注册人传真 + 分机	域名控制 域名认证 企业域名购买/销售* 学术/公众利益 DNS 研究* 法律诉讼* 监管/合同的执行
注册人可能选择公布的新联系方式： 注册人 SMS 注册人 IM 注册人社交媒体 注册人备用社交媒体 注册人联系人 URL 注册人滥用 URL	可用于每一种容许目的 作为注册人电子邮件地址的备选项
管理联系人 ID 管理联系人数据元素	域名控制 域名认证 企业域名购买/销售 学术/公众利益 DNS 研究 DNS 透明度
法务联系人 ID 法律联系人数据元素	域名控制 域名认证 学术/公众利益 DNS 研究 法律诉讼 监管/合同的执行 DNS 透明度
技术联系人 ID 技术联系人数据元素	域名控制 解决技术问题 域名认证 学术/公众利益 DNS 研究 DNS 透明度
滥用问题联系人 ID 滥用问题联系人数据元素	域名控制 域名认证 学术/公众利益 DNS 研究 犯罪调查/减少 DNS 滥用 DNS 透明度
隐私/代理联系人 ID 隐私/代理服务提供商联系人数据元素	域名控制 个人数据保护 域名认证 学术/公众利益 DNS 研究 DNS 透明度
业务联系人 ID 业务联系人数据元素	域名控制 域名认证 个人互联网使用 学术/公众利益 DNS 研究 DNS 透明度
DNSSEC 授权	域名控制 学术/公众利益 DNS 研究

数据元素	目的
注册状态 客户端状态（注册服务商） 服务器状态（注册管理机构）	域名控制 企业域名购买/销售 学术/公众利益 DNS 研究 监管/合同的执行 犯罪调查/减少 DNS 滥用
注册服务商 分销商 注册服务商 URL 注册服务商 IANA 号码 注册服务商滥用问题联系人电子邮件地址 注册服务商滥用问题联系人电话号码 Internic 投诉站点 URL	域名控制 企业域名购买/销售 学术/公众利益 DNS 研究 监管/合同的执行 犯罪调查/减少 DNS 滥用 DNS 透明度
注册服务商所在辖区 注册管理机构所在辖区 注册协议语言	所有
原始注册日期	域名控制 企业域名购买/销售 学术/公众利益 DNS 研究 监管/合同的执行
创建日期 更新日期 注册服务商到期日期	域名控制 企业域名购买/销售 学术/公众利益 DNS 研究 监管/合同的执行 犯罪调查/减少 DNS 滥用

注：以上带 * 标记的用途有时需要访问网关注册人数据元素，这可能涉及“须知”审批；请参阅第 III 部分，了解“批准的网关数据”的讨论。

附录 E：演示网关和未经身份验证访问

以下注册数据记录针对 2013 RAA WHOIS 示例进行了扩展，以体现为数据的收集和披露而建议的 RDS 原则。

灰色元素为可选元素；其他为必需的元素。
粗体元素始终为公共元素；其他可能为网关元素，这取决于注册人或联系信息持有者的选择。

注册状态：x **DNSSEC 授权：signedDelegation** **客户端状态：DeleteProhibited（禁止删除）、RenewProhibited（禁止续用）、TransferProhibited（禁止迁移）** **服务器状态：DeleteProhibited（禁止删除）、RenewProhibited（禁止续用）、TransferProhibited（禁止迁移）** **注册服务商：EXAMPLE REGISTRAR LLC** **分销商：示例分销商** **注册服务商管辖区：示例管辖区** **注册管理机构管辖区：示例管辖区** **注册协议语言：英语** **创建日期：2000-10-08T00:45:00Z** **原始注册日期：2000-10-08T00:45:00Z** **注册服务商注册到期日期：2010-10-08T00:44:59Z** **更新日期：2009-05-29T20:13:00Z** **注册服务商 URL：http://www.example-registrar.tld** **注册服务商 IANA 号码：5555555** **注册服务商滥用问题联系人电子邮件：email@registrar.tld** **注册服务商滥用问题联系人电话：+1.1235551234** **Internic 投诉站点 URL：http://wdprs.internic.net/**	由注册管理机构或注册服务商提供
域名：EXAMPLE.TLD **域名服务器：NS01.EXAMPLE-REGISTRAR.TLD** 注册人姓名：示例注册人 **注册人类型：法人** **注册人联系人 ID：xxxx-xxxx**（由 RDS 委任的验证方签发） **注册人联系人验证状态（来自验证方）** **注册人联系人上次验证时间戳（来自验证方）** 注册人组织：示例组织	从注册人处收集

注册人公司标识符：D-U-N-S #12345（由 Dunn 和 Bradstreet 签发） **注册人电子邮件：EMAIL@EXAMPLE.TLD** 注册人备用电子邮件：EXAMPLE@OTHERDN.TLD 注册人街道：123 EXAMPLE STREET 注册人所在城市：ANYTOWN 注册人所在州/省：AP 注册人邮编：A1A1A1 **注册人所在国家/地区：AA** 注册人电话：+1.5555551212 注册人电话分机号：1234 注册人备用电话：<cellnumber> 注册人备用电话分机：1234 注册人传真：+1.5555551213 注册人传真分机号：4321 注册人 SMS：<textingnumber> 注册人 IM：<IMhandle> 注册人社交媒体：<SMhandle> 注册人备用社交媒体：<OtherSMhandle> 注册人联系人 URL：<“与我联系”表单或说明的链接> 注册人联系人 URL：<“滥用报告”表单或说明的链接>	
管理员联系人 ID：xxxx-xxxx **（后接管理 PBC 联系详细信息*）**	注册人必须发布基于目的的联系人针对必需的 PBC 类型
技术联系人 ID：xxxx-xxxx **（后接技术 PBC 联系详细信息*）**	
法律联系人 ID：xxxx-xxxx **（后接法律 PBC 联系详细信息*）**	
滥用问题联系人 ID：xxxx-xxxx **（后接滥用问题 PBC 联系详细信息*）**	
业务联系人 ID：xxxx-xxxx（仅当注册人类型 = 法人时） （后接企业 PBC 联系详细信息*）	
隐私/代理联系人 ID：xxxx-xxxx（仅当注册人类型 = 隐私/代理服务提供商时） （后接 PP 提供商 PBC 联系详细信息*）	

图例： 灰色元素为可选/有条件收集的元素；其他为必需的元素。
粗体元素始终为公共元素；其他可能为网关元素，这取决于注册人或联系信息持有者的选择。* 此处未详细说明 PBC 数据元素。

示例 #1：用于解决技术问题的未经身份验证的公开查询

1) 用户提交未经身份验证的 RDS 查询
（DN = MerchantZ.gtld、目的 = 解决技术问题、数据 = 所有）

2) RDS 评估查询：
未通过身份验证，因为查询未经身份验证
未授权，因此授予公共数据的访问权限
限定为访问用于解决技术问题的公共数据 —
也就是说，所有为域名和技术联系人而请求的公共数据

3) RDS 检索请求的数据元素：
从 RDS 缓存（同步）中检索 MerchantZ.gtld 数据，或注册管理机构（联合）
仅交付为此目的定义的公共数据元素，包括：

注册人联系人 ID = 12345
注册人类型 = 法人
注册人组织 = MerchantZ, Inc.[38]
技术联系人 ID = 67890

技术联系人 ID [67890] 从 RDS 缓存中或验证方处检索，仅获取该联系人为此目的明确发布的公共数据元素，包括

PBC ID = 67890

PBC 名称 = <*负责为域名 MerchantZ.gtld 解决技术问题的实体的名称*>

PBC 电子邮件地址 = <*负责为域名 MerchantZ.gtld 解决技术问题的实体的必需电子邮件地址*>

PBC 备用电子邮件地址 = <*负责为此域名解决技术问题的实体的建议备用电子邮件地址*>

PBC 电话号码 = <*负责为此域名解决技术问题的实体的建议电话号码*>

PBC 联系人 URL= <*负责为此域名解决技术问题的实体发布的建议联系人链接*>

<*此实体发布的任何可选公共数据元素*>

[38] 注册人组织从将“注册人类型”设置为“法人”的注册人或委任的隐私/代理服务提供商处收集；如果“注册人类型”默认为“未申报”，则可能不提供该组织

4) RDS 向用户返回错误条件或成功响应。例如：

域名：MerchantZ.gtld *注册状态：x* *客户端状态：DeleteProhibited、RenewProhibited、TransferProhibited* *服务器状态：DeleteProhibited、RenewProhibited、TransferProhibited* *注册服务商：EXAMPLE REGISTRAR LLC* *注册服务商管辖区：示例管辖区* *注册管理机构管辖区：示例管辖区* *注册协议语言：英语* *创建日期：2000-10-08T00:45:00Z* *注册服务商注册到期日期：2010-10-08T00:44:59Z* *更新日期：2009-05-29T20:13:00Z* *注册服务商 URL：* *http://www.example-registrar.tld* *注册服务商 IANA 号码：5555555* *注册服务商滥用问题联系人电子邮件：email@registrar.tld* *注册服务商滥用问题联系人电话：+1.1235551234* *Internic 投诉站点 URL：http://wdprs.internic.net/*
域名服务器：NS01.EXAMPLE-REGISTRAR.TLD *注册人联系人 ID = 12345* *注册人类型 = 法人* *注册人组织 = MerchantZ, Inc.* *注册人电子邮件 = 12345@MerchantZ.gtld* *注册人联系人验证状态 = 操作验证* *注册人联系人上次验证时间戳 = x* *<注册人为此域名发布的其他可选公共数据元素>*
技术联系人 ID = 67890 *PBC ID = 67890* *PBC 验证状态 = 操作验证* *PBC 上次验证时间戳 = x* *PBC 名称：示例技术员* *PBC 电子邮件 = mailto:67890@MerchantZ.gtld* *PBC 备用电子邮件 = SuperbHostingServices@OtherDN.gtld* *PBC 电话号码 = +1.1235567890* *PBC 联系人 URL = TechSupport@SuperbHostingServices.gtld* *<此 PBC 发布的可选公共数据元素>*

示例 #2：用于解决技术问题的通过身份验证的网关查询

1) 用户提交通过身份验证的 RDS 查询
（DN = PersonY.gtld、目的 = 解决技术问题、数据 = 所有）

2) RDS 评估查询：
- 如果“A”可信，则批准网关查询。
- 如果“A”是委任的 ISP，则授予用于解决技术问题的访问权限
- 限定为访问解决技术问题所需的公共和网关数据
- 限定为访问解决技术问题所需的公共和网关数据 — 也就是说，所有为此目的和技术联系人而请求的公共和网关数据

3) RDS 检索请求的数据元素：
从 RDS 缓存（同步）中检索 PersonY.gtld 数据，或注册管理机构（联合）获取为此目的定义的公共和网关数据元素，包括：

注册人联系人 ID = 12345
注册人类型 = 未申报
<此注册人发布的任何可选公共或网关数据元素 — 例如，他/她的姓名（如果注册人选择）>
技术联系人 ID = 67890[39]

技术联系人 ID [67890] 从 RDS 缓存中或验证方处检索，获取该联系人为此目的明确发布的公共和网关数据元素，包括

PBC ID = 67890

PBC 电子邮件地址 = <*负责为域名 PersonY.gtld 解决技术问题的实体的必需电子邮件地址*>

PBC 备用电子邮件地址 = <*负责为此域名解决技术问题的实体的建议备用电子邮件地址*>

PBC 电话号码 = <*负责为此域名解决技术问题的实体的建议电话号码*>

PBC 联系人 URL = <*负责为此域名解决技术问题的实体发布的建议联系人链接*>

<*此实体发布的任何可选公共或网关数据元素 — 例如，SMS 号码*>

[39] 如果注册人在注册域名期间未提供任何联系人 ID，则应告知注册人，会将注册人自己的地址发布为主要 PBC（并为其提供表示同意的机会），以提供另一个主要 PBC ID（例如，隐私服务提供商的联系人 ID），或取消注册。

4) RDS 向用户返回错误条件或成功响应。例如：

域名：PersonY.gtld *注册状态：x* *客户端状态：DeleteProhibited、RenewProhibited、TransferProhibited* *服务器状态：DeleteProhibited、RenewProhibited、TransferProhibited* *注册服务商：EXAMPLE REGISTRAR LLC* *注册服务商管辖区：示例管辖区* *注册管理机构管辖区：示例管辖区* *注册协议语言：英语* *创建日期：2000-10-08T00:45:00Z* *注册服务商注册到期日期：2010-10-08T00:44:59Z* *更新日期：2009-05-29T20:13:00Z* *注册服务商 URL：http://www.example-registrar.tld* *注册服务商 IANA 号码：5555555* *注册服务商滥用问题联系人电子邮件：email@registrar.tld* *注册服务商滥用问题联系人电话：+1.1235551234* *Internic 投诉站点 URL：http://wdprs.internic.net/*
域名服务器：NS01.EXAMPLE-REGISTRAR.TLD *注册人联系人 ID = 12345* *注册人类型 = 未申报* *注册人电子邮件 = 12345@PersonY.gtld* *注册人联系人验证状态 = 操作验证* *注册人联系人上次验证时间戳 =x* *<注册人为域名发布的其他可选公共或网关数据元素，如：注册人姓名或注册人 SMS 或注册人联系人 URL>*
技术联系人 ID = 67890 *PBC ID = 67890* *PBC 验证状态 = 操作验证* *PBC 上次验证时间戳 = x* *PBC 名称：示例技术员* *PBC 电子邮件 = 67890@SuperbHostingServices.gtld* *PBC 备用电子邮件 = SuperbHostingServices@OtherDN.gtld* *PBC 电话号码 = +1.1235567890* *PBC 联系人 URL = TechSupport@SuperbHostingServices.gtld* *<此 PBC 发布的可选公共或网关数据元素>*

示例 #3：为域名购买/销售或法律诉讼批准的网关数据查询

调查可能的商标侵权行为的过程如下所述，但类似的起点和步骤也适用于域名购买、合并/收购以及出于这些和其他目的的许多其他调查。

步骤 1)：RDS 用户登录到委任机构（如第 IV(c) 部分：RDS 用户委任所定义），并证实不仅他们的目的是法律诉讼，而且所获取的数据用于调查主体“X”的可能商标侵权行为。用户提供作为利益主体的个人/组织的名称和联系信息。因此，此目的的 RDS 查询在本质上限定为与该主体关联的注册数据。

步骤 2)：然后，RDS 用户可能会对有关该主体的已知值执行反向查询，在 RDS 中搜索包括给定值的域名列表，例如：

- 注册人和/或 PBC 名称/组织
- 注册人和/或 PBC 电话/备用电话
- 注册人和/或 PBC 邮政地址，或
- 注册人和/或 PBC 电子邮件/备用电子邮件

这其中的一些数据元素可能为网关数据。反向查询将搜索这些批准的网关数据元素，但仅限于给定值和规定的目的（如证明文件中所述）。

步骤 3)：给定正在调查的域名列表（这些域名可能涉及正在调查的商标侵权行为）后，RDS 用户现在可以对那些域名执行 RDS 查询，以获取评估案例所需的数据，主要包括：

- 联系人 ID
- 注册日期
- 注册服务商所在辖区
- 注册管理机构所在辖区
- 注册人所在国家/地区（注册人的管辖区）
- 注册人组织，以及
- 注册人公司标识符

为这些域名进行 WhoWas 查询也可能请求上述相同的信息。在此步骤中，除一个元素外，所有数据元素都是公共元素；唯一的网关数据是“注册人所在国家/地区”。

步骤 4)：在得出结论，确定适合采取进一步行动后，RDS 用户可以执行 RDS 查询来检索已发布的公共法律联系人 ID 和关联的联系数据（包括 PBC 名称/组织、电话和邮政地址）。这些结果可用于尝试联系注册人的指定法律联系人，或用于提起诉讼、进行 UDRP 申诉或采取其他法律行动。

步骤 5)：如果法律联系人拒绝对域名承担责任，则可能需要注册人的完整联系详细信息才能采取法律行动。在步骤 1 中可能已经获知了这其中的大多数数据，但未从 RDS 中获取。不过，此时可能存在一些需要弥补的差距。

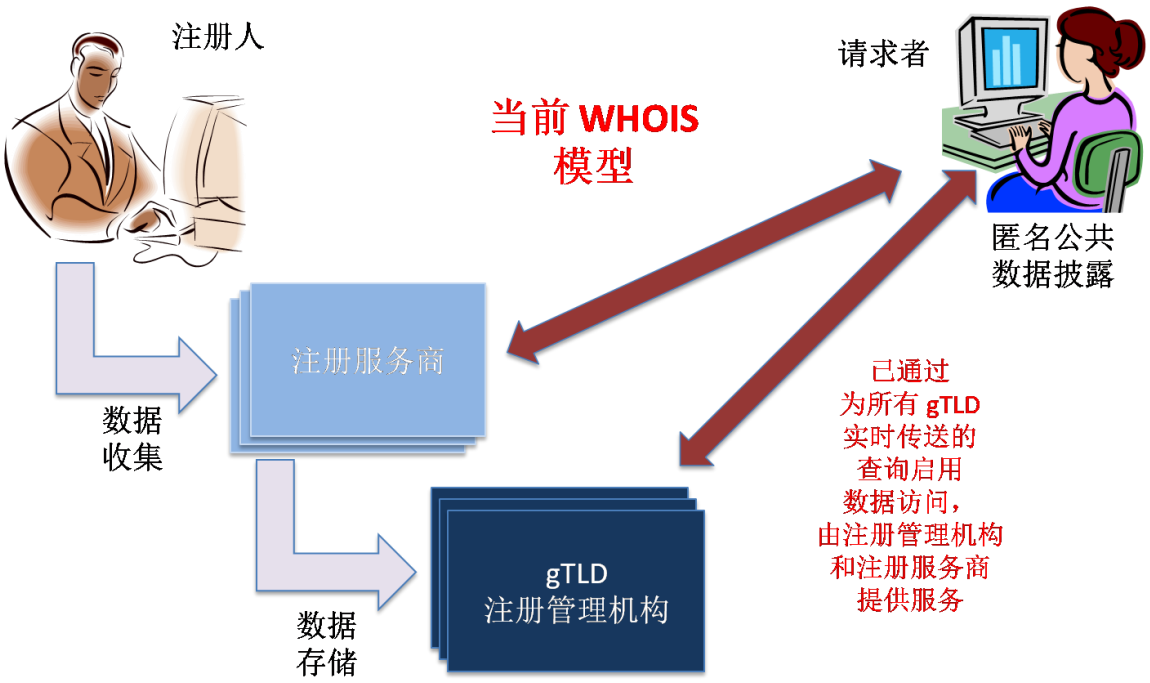
此示例说明了可能涉及与商标侵权相关的调查和可能的法律行动的 RDS 交互。但是，在其他类型的法律行动中以及在购买/销售期间调查域名资产时，也可能发生一系列非常类似的步骤。如果涉及批准的网关数据，则委任方应负责审核访问以检测可能超出声称的有限范围的请求，同时负责采取步骤以阻止滥用和执行 ToC。将 RDS 用户的证明文件存档将有助于委任方审核访问并调查可能的滥用情况。它还可用于制止非法调查。

附录 F：考量的系统模型和方法

除了之前在可能的 DS 模型中介绍的模型外，EWG 还考量了以下备选模型，但发现每个模型的可行性要低于联合或同步模型，理由如下。

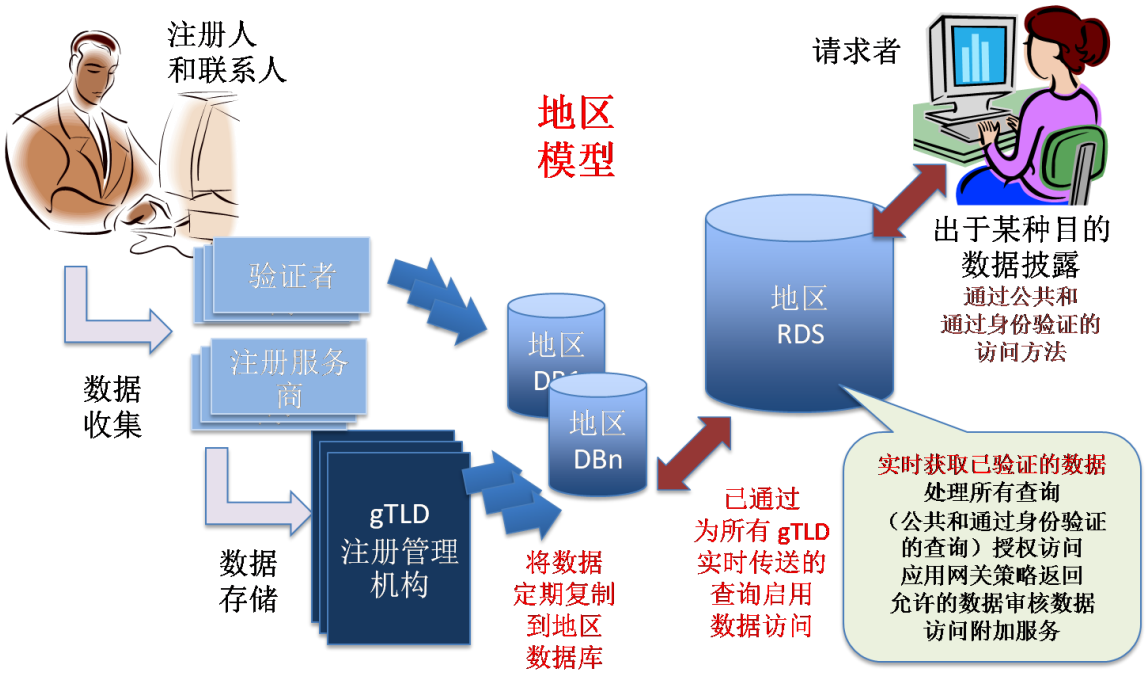
当前 WHOIS

此模型介绍当前的 WHOIS 系统采用的完全分散的自治方法，即注册管理机构和注册服务商提供它自己的 WHOIS 服务，而不在所有 gTLD 之间进行集成。虽然可以建立一个集中式门户以便在所有 gTLD 之间访问 WHOIS，但每个注册管理机构仍然直接（详细）或通过向注册服务商授权（简略）来提供它自己的独立管理的存储和访问。



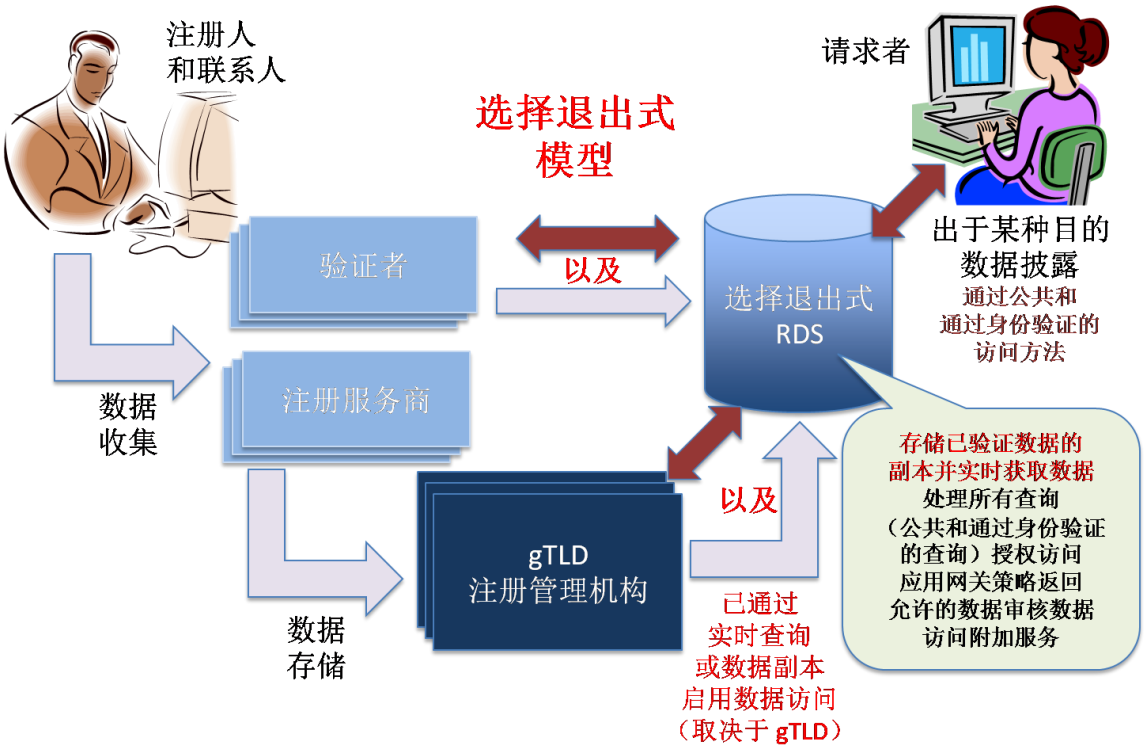
地区模型

此模型介绍了这样一个 RDS：它定期将数据从注册管理机构和验证方运营的分布式存储区复制到位于全球各地的地区存储区。注册管理机构和验证方将继续存储数据，但该 RDS 可使用数据的地区副本更高效地处理访问请求。地区存储区由该 RDS 运营，但受每个存储区所在管辖区的法律制约。



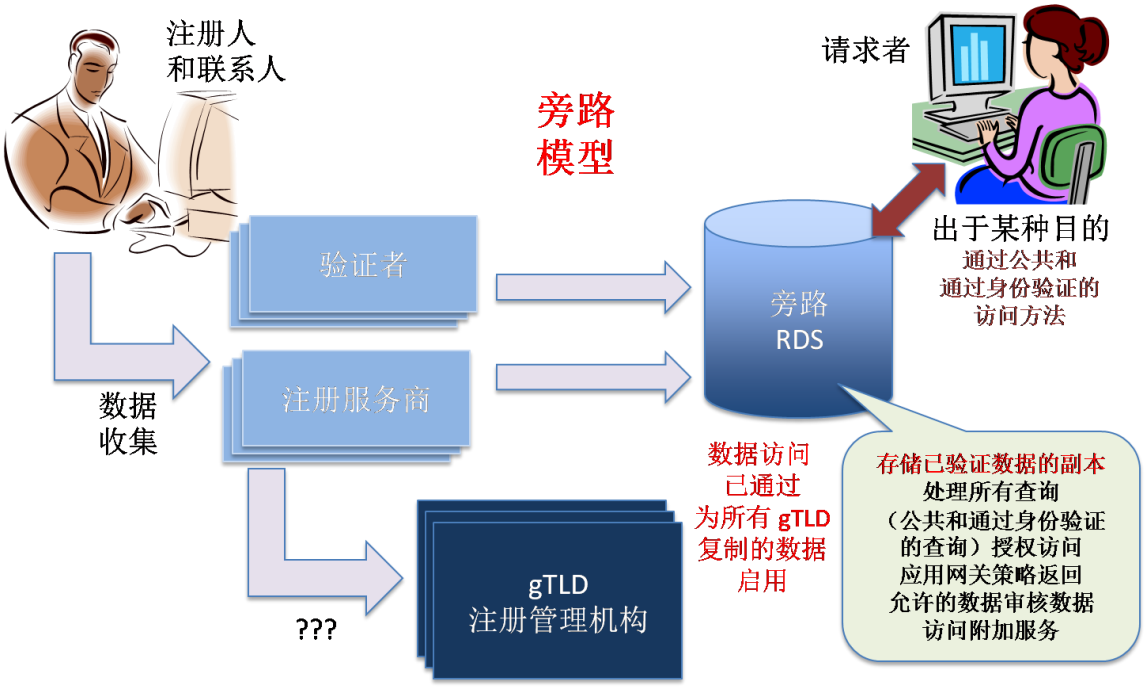
选择退出式模型

此模型介绍了这样一个 RDS：它定期将数据从由注册管理机构运营的分布式存储区复制到该 RDS 运营的同步存储中。在此模型下，任何注册管理机构均可以选择退出同步存储，只要它们同意根据可用性和性能服务水平协议 (SLA) 提供必要的基础架构来处理所需的重要查询。



旁路模型

此模型介绍了这样一个 RDS：它定期将数据从由注册服务商运营的分布式存储区复制到该 RDS 运营的同步存储中。在此模型下，将不考虑将注册管理机构作为注册信息源；RDS 服务查询使用直接复制自权威来源的同步注册数据。



用于比较系统模型的方法

EWG 考量了当前 WHOIS 系统固有的随附成本和安全缺陷，记录 WHOIS 缺陷的附录 B 中列出的报告介绍了其中许多成本和缺陷。EWG 比较了当前 WHOIS 系统的成本和缺陷与可能模型的对应项的异同。此外，EWG 还根据以下标准比较了每一种可能的模型的安全性优缺点：

安全性影响

- **单一故障点：**考虑到使用了分布式体系结构和主要服务提供商，该模型承受任何单一系统故障的能力如何？任何系统临时故障是否会导致无法访问所有或仅部分注册信息？**注：**应采用合理的数据库设计和操作实践来提供内部冗余和数据备份，因此，这实际上与故障期间的数据可用性有关。
- **遭受内部滥用：**该模型阻止内部人员滥用，即管理/操作人员访问作为模型一部分的任何系统予以存储或通过其传送的注册数据的能力如何？内部人员滥用是否会导致可未授权访问所有或部分数据？应用控制来检测/阻止内部人员滥用的难易程度如何？
- **遭受外部攻击：**该模型抵御针对作为模型一部分的任何系统的外部攻击的能力如何？外部攻击是否会导致侵犯所有或部分注册人的隐私？应用控制来检测/阻止外部攻击的难易程度如何？
- **安全一致性：**该模型接受不一致的安全实施和政策执行的能力如何？负责运营系统组件的所有参与者是否能够一致地实现安全性目标？或者，注册服务商/注册管理机构/验证方专业技能和投资方面的差异是否会对安全性造成重大影响？

管辖区和隐私影响

- **在当地管辖区中存储数据：**该模型是否允许将注册信息存储在多个管辖区之一？注册服务商或注册管理机构/验证方可在多大程度上选择将注册信息存储在具有与注册人的当地管辖区相一致的数据保护法的管辖区？
- **支持应用当地法律来显示：**该模型是否允许以与多个管辖区之一相一致的方式访问注册信息？该 RDS 可在多大程度上对通过 RDS 访问的注册信息应用注册人当地管辖区的数据保护法？
- **支持遵守当地数据保护法：**该模型是有助于还是不利于注册服务商和注册管理机构遵守对它们适用的当地数据保护法？该模型在何种程度上增加了获取确保合规性所需异常的繁琐程度？如何确保遵守注册人的当地法律规定的法律程序？

委任

- **支持请求者委任：**该模型是否允许希望出于某种目的而访问网关数据的用户申请委任、接受审查、接收访问凭证并使用这些凭证获得相应的授权来访问数据？该模型可在多大程度上有助于或不利于一致而可靠地应用此类请求者委任流程？

  验证：它是否使验证更加简单？它是否会降低验证的成本？是否有任何系统使安全凭证更简单或成本更低廉？

- **跟踪/惩罚请求者：**该模型为检测对委任访问的滥用（即，违反访问条款和条件的行为）而记录数据访问请求和响应的效率和可靠性如何？该模型可在多大程度上有助于或不利于采取合规性执行措施（即，对不合规的用户进行惩罚来阻止将来的滥用情况）？

- **审核：**该模型是否支持审核数据访问请求和响应以及相关操作，以评估委任流程和授权数据访问的效率？

操作

- **用户友好的门户：**该模型是否允许以用户友好的方式提供通过 Web 门户显示或在协议查询响应中返回的注册信息？该模型可在多大程度上支持国际化原则（即，支持本地字符集、响应翻译）？该模型可在多大程度上促进所有 gTLD 间的一致显示？

- **随机数据审核/准确性报告：**该模型是否支持定期在所有 gTLD 之间进行准确性审核和准确性报告？该模型可在多大程度上促进高效、一致地检测和更新不准确的注册信息以及统一执行准确性政策？

- **数据延迟（性能）：**该模型是否在数据处理方面存在效率低下的固有缺陷，这可能会导致性能降低，并且无法通过实施可扩展平台来解决？在处理请求的速度和查询注册数据的用户意识到的延迟方面，那些低效现象的相对大小是多少（与其他模型相比）？

- **数据同步：**该模型是否要求将从任何系统复制的数据与其他系统同步？这些数据同步需要的广泛程度如何？任何临时缺乏同步问题的严重程度如何（与其他模型相比）？

- **注册人访问自己的数据：**该模型是支持还是会阻止注册人访问他/她自己的注册数据？

- **存储/托管要求：**该模型是否引入了多个存储区，增加了数据存储和托管要求的数量或复杂性？

- **支持预验证措施：**该模型是否支持对所有 gTLD 之间的注册人和基于目的的联系人信息进行预验证？该模型可在多大程度上促进高效、一致地创建和维护预验证的联系信息以及统一执行任何相关唯一性政策？

实施

- **复杂基础架构：**与其他模型相比，该模型总体上的复杂程度是否更低？例如，更加复杂（更加薄弱）的模型可能包含更多需要初始投资和持续维护的系统和接口。
- **易于实施：**与其他模型相比，该模型是否更易于实施？例如，更加繁琐（更加薄弱）的模型可能需要对更多系统做出更改。
- **易于过渡：**与其他模型相比，该模型会在多大程度上支持从当前的 WHOIS 平稳过渡到下一代 RDS？在这方面，更加薄弱的模型指使用户、注册服务商和注册管理机构更难以从现有流程过渡的模型。

成本

- **降低注册服务商和注册管理机构的 WHOIS 运营成本：**与当前的 WHOIS 系统相比，该模型是否会降低注册服务商和注册管理机构的持续运营和维护成本？在这方面，可降低成本的模型更强大。
- **降低实施成本：**与其他模型相比，该模型在新的/修改后的基础架构和流程方面需要的总体初始投资是更多还是更少？在这方面，总体实施成本更低的模型更强大。
- **反向查询和历史 WhoWas：**该模型是否需要额外的投资来支持授权请求者的反向查询和历史 WhoWas 搜索？在这方面，提供这些服务所需的总体成本越低，模型越强大。

使用案例

比较这些可能的模型支持在初步报告中确定的所有用户和目的的能力，包括（但不限于）以下 gTLD 使用案例：

- 域名收购
- 域名注册历史记录（包括跟踪任何域名的注册历史记录 (WhoWas)）
- 指定注册人注册的域名（包括查找特定注册人注册的每个域名[反向 RDS 查询]）
- UDRP 程序
- 调查遭到滥用的域名
- 阻止互联网恶意活动

模型成本分析

为分析与 SRDS 和 FRDS 模型关联的实施可行性和成本，ICANN 请 IBM 以这两个可能的实施模型之间的成本差异为重点进行了详细分析。IBM 编制了名为“*注册目录服务 (RDS) 实施模型成本分析*[40]”的最终报告。此处转载了该报告中 IBM 分析结果的摘录以供参考。

方法

2014 年 2 月/3 月进行了一次预算成本分析，比较了实施同步[41] *和联合 RDS 的实际情况。采用的分阶段方法如下所述：*

- *步骤 1：为每一个实施模型收集基准要求。*
- *步骤 2：定义关键度量假设（由 ICANN 提供并在很大程度上基于 gTLD 注册管理机构提交的每月 WHOIS 查询报告）并就此达成一致 使用这些假设推导预计的系统工作负载，并为两个实施模型分别定义高级基准解决方案概要。*
- *步骤 3：创建成本模型，然后对每个基准解决方案概要执行成本预算。*
- *步骤 4：编制分析结果。*

出发点

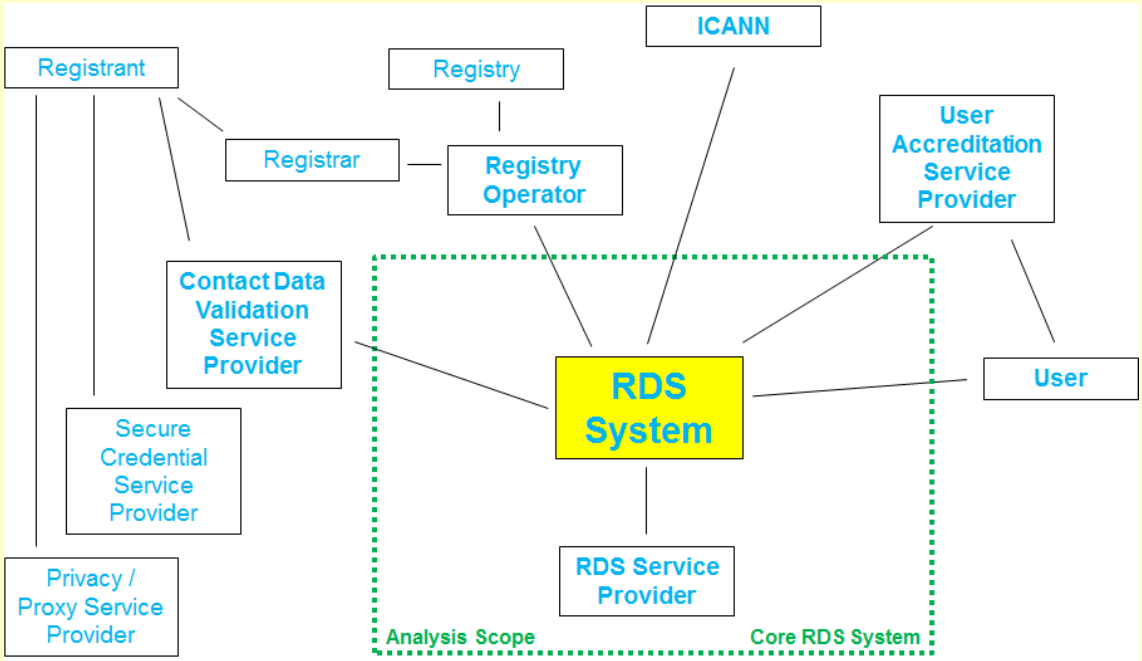
- *为中央“RDS 系统/提供商”创建预算成本估算。不估算注册管理执行机构的成本。*
- *创建托管服务成本模型和估算。也就是说，假定设置和持续运营托管 RDS 服务并估算相关成本。*
- *为进行成本比较，解决方案和成本在很大程度上基于 IBM 的产品组合（主要为 IBM 的 SoftLayer IaasS 产品），仅在 IBM 产品组合中没有替代产品的情况下才使用第三方解决方案组件。*
- *只为基准要求/解决方案概要、而不为变体创建成本估算；不进行详细的成本驱动因素分析。*

[40] https://community.icann.org/display/WG/EWG+Public+Research+Page

[41] 为了与 EWG 的最终报告保持一致，本摘要将早期 EWG 报告中介绍的集中式 RDS (ARDS) 模型称为同步 RDS (SRDS)。

核心分析范围和度量标准

成本分析的重点为“核心 RDS 系统”，如下所述



在每个模型（同步和联合）中定义了要支持的核心使用案例。

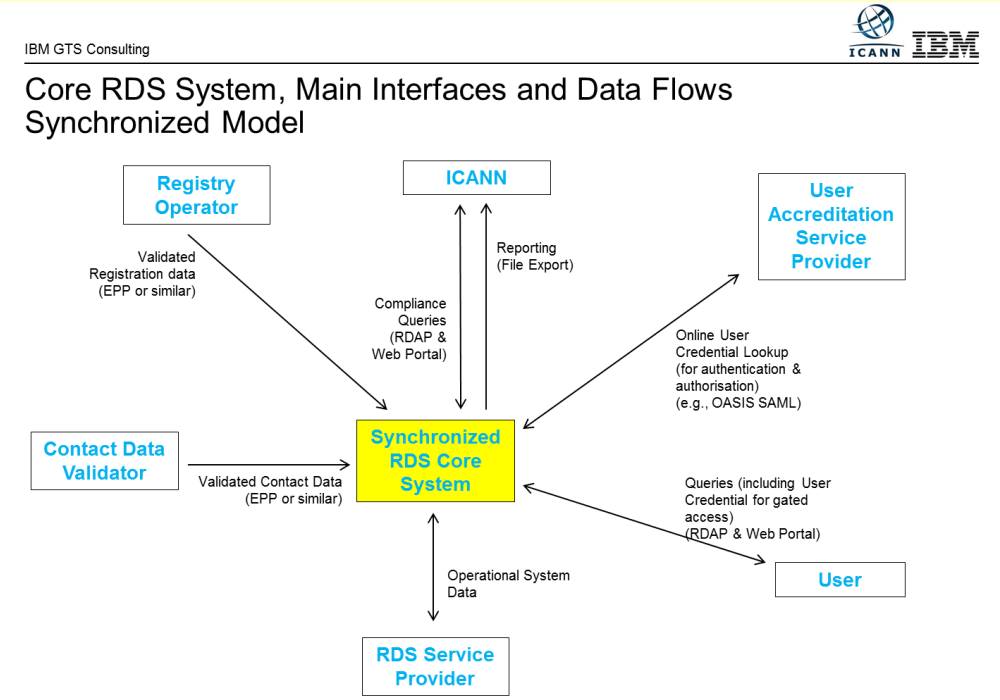
此外还定义了关键度量假设：

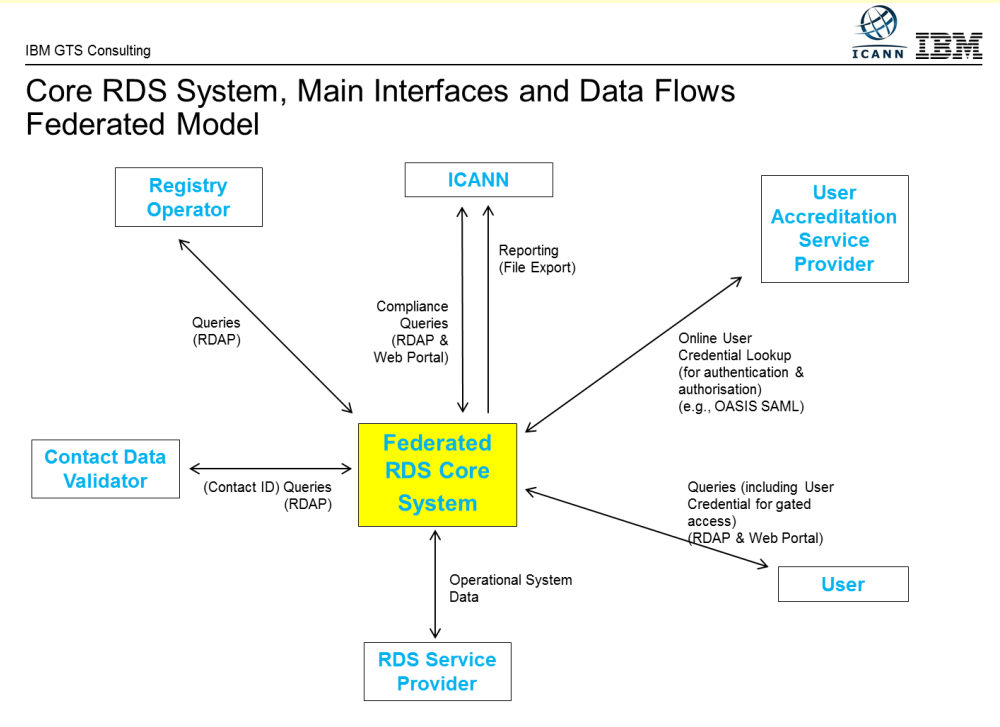
YEARLY GROWTH RATE	22%	nr of DN records added in a year, assumed to include the growth in the nr of gTLDs					
Nr of DN RECORDS, YEARLY UPDATE RATE	100%	nr of DN records updated in a year					
		start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
Nr of gTLDs		2000	3000	4000	5000	6000	7000
growth rate			50%	33%	25%	20%	17%
	December 2013, ICANN input	start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
NR OF DOMAIN NAMES	151.196.101	184.459.243	225.040.277	274.549.138	334.949.948	408.638.936	498.539.502
NR OF QUERIES/MONTH	9.031.522.529	11.018.457.485	13.442.518.132	16.399.872.121	20.007.843.988	24.409.569.665	29.779.674.992
AVERAGE NR OF QUERIES/SEC	3.484	4.251	5.186	6.327	7.719	9.417	11.489
NR OF QUERIES/PEAK SEC		42.509	51.862	63.271	77.191	94.173	114.891
AVERAGE NR OF QUERIES/HOUR	12.543.781	15.303.413	18.670.164	22.777.600	27.788.672	33.902.180	41.360.660
NR OF QUERIES IN PEAK HOUR	25.087.563	30.606.826	37.340.328	45.555.200	55.577.344	67.804.360	82.721.319
USER VISITS IN PEAK HOUR	16.892.292	20.608.596	25.142.488	30.673.835	37.422.079	45.654.936	55.699.022
CONCURRENT VISITS IN PEAK HOUR	563.076	686.953	838.083	1.022.461	1.247.403	1.521.831	1.856.634
NEW VISITS IN PEAK SEC		28.623	34.920	42.603	51.975	63.410	77.360

% of reverse queries	1,0%

RDS 实施模型

以下实施模型来自 EWG 为进行成本分析而提交的初步报告和状态更新报告：



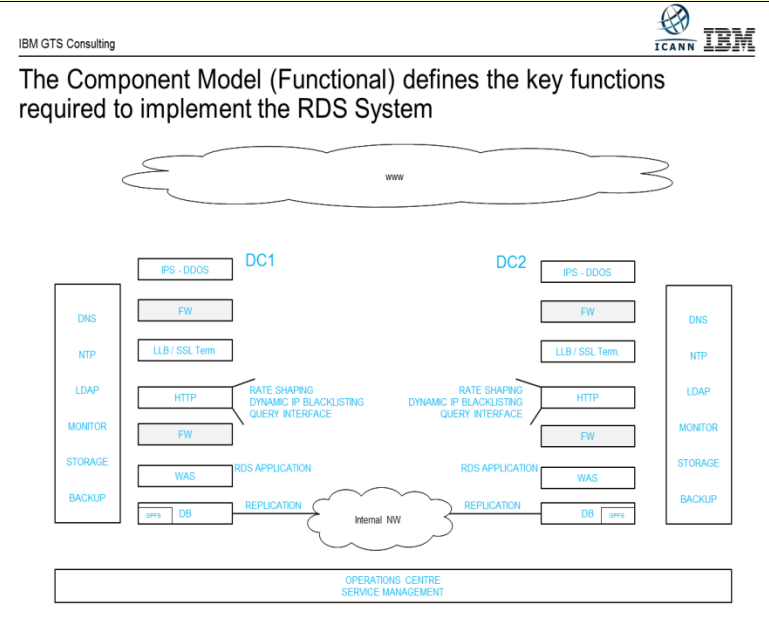


RDS 功能组件

为进行成本分析，创建了以下组件模型，在此过程中组合了实施 RDS 系统所需的关键功能。在估算 SRDS 和 FRDS 的成本时使用了标准系统设计最佳实践假设，如在两个不同地域的数据中心之间复制 RDS 核心系统和数据库，通过负载均衡和故障切换确保冗余和可用性，通过 IPS 防御 DDoS。应该了解的是，这些功能组件适用于上述两个实施模型。

功能组件：

- *数据中心间的负载均衡/路由*
- *IPS DDoS 防御*
- *数据中心内的负载均衡和 SSL*
- *Web (HTTP) 服务器*
- *Web 应用程序服务器 (WAS)*
- *WAS 管理节点*
- *数据库 (DB) 缓存系统*
- *DB 成员系统*
- *存储服务器*
- *系统监控*
- *DNS*
- *NTP*
- *LDSP*
- *系统日志存储库*
- *备份服务器*
- *备份存储服务器*
- *DB 备份客户端系统*
- *网络分区、防火墙/IPS*
- *互联网和数据中心连接*



例如，为 SRDS 和 FRDS 模型中的核心 RDS 系统假定了双数据中心设置，如果每个核心 RDS 能够处理 50% 的峰值负载，则使用双主动设计。此成本分析不包括为在每个数据中心内实现高可用性而进行聚集；可以增加此功能，而不更改两个 RDS 模型的相对成本。

成本估算（假定反向查询占 1%）

*下面汇总的成本估算决不构成 IBM 实施建议。进行成本估算的唯一目的，只是为了在预算成本分析时使用和考量，从而对两个 RDS 实施模型进行比较。根据上述关键度量标准、工作负载要求和解决方案概要，**仅核心 FRDS 和 SRDS 系统**中每个域名每年的成本估算如下：*

SRDS 预算成本估算

€	0,0183	average cost/domain/year			
cost per domain name					
yr1	yr2	yr3	yr4	yr5	
€ 0,041	€ 0,023	€ 0,017	€ 0,020	€ 0,019	

FRDS 预算成本估算

€	0,0173	average cost/domain/year			
cost per domain name					
yr1	yr2	yr3	yr4	yr5	
€ 0,041	€ 0,018	€ 0,017	€ 0,021	€ 0,017	

对成本差异所做的进一步分析和比较如下：

FRDS – SRDS Budgetary Cost Estimate Differences

SETUP COSTS		**5,9%**		10,5%	
INFRASTRUCTURE SETUP COSTS	ARCHITECTURE & DESIGN	**1,5%**	0,2%	15,6%	0,0%
	PROVISION & CONFIGURE		1,2%		19,2%
	INFRASTRUCTURE TESTING		0,1%		18,4%
APPLICATION SETUP COSTS	ANALYSIS, DESIGN, CODE, UNIT TEST	**1,2%**	1,2%	0,0%	0,0%
TESTING	INTEGRATION TESTING & DEPLOYMENT	**1,7%**	0,8%	7,8%	0,0%
	E2E SYSTEM TESTING		0,2%		38,2%
	PERFORMANCE		0,2%		33,3%
	SECURITY (ETHICAL HACK)		0,5%		0,0%
TRANSITION TO BAU	TRANSITION TO BAU	**0,6%**	0,5%	26,6%	37,7%
	SERVICE DESK SETUP		0,1%		0,0%
MANAGEMENT	PROJECT MANAGEMENT	**0,9%**	0,9%	13,4%	13,4%

The FRDS model implies a higher computing power requirement (more systems required to handle the envisaged load) in the web and web application server layer.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve more testing effort

FRDS – SRDS Budgetary Cost Estimate Differences

COST MODEL FRDS		SHARE IN TOTAL		DIFFERENCE WITH ARDS	
		100,0%		-5,4%	
RUN COSTS		94,1%		-6,3%	
INFRASTRUCTURE COSTS	PUBLIC NW	**30,5%**	8,1%	-22,4%	-55,9%
	DC NW, GLB, LLB, IPS/DDOS		5,7%		10,7%
	HTTP SERVERS		2,2%		236,0%
	WAS SERVERS		3,7%		218,5%
	DB SERVERS		2,2%		-52,0%
	STORAGE		6,3%		-3,8%
	BACKUP		1,9%		-19,0%
	GENERIC SYSTEMS		0,3%		0,0%
SW LICENCE & MAINTENANCE COSTS	DB	**32,7%**	13,7%	-17,5%	-59,5%
	WAS		18,8%		234,6%
	BACKUP		0,3%		0,0%
OPERATIONS AND MANAGEMENT COSTS	INFRA OPERATIONS & MAINTENANCE	**30,9%**	19,4%	44,0%	63,6%
	APPLICATION OPERATIONS		2,6%		20,0%
	APPLICATION MAINTENANCE		1,3%		27,3%
	SERVICE GOVERNANCE		5,2%		0,0%
	SERVICE DESK		2,4%		100,0%

The Public NW cost is lower in the FRDS case due to the IBM SoftLayer NW charging model: incoming traffic is free; per server 20 TB/month outgoing traffic is free, i.e. you get a total free outgoing volume of #servers x 20 TB per month. As the number of servers increases in the FRDS model, the total amount of free TB outgoing NW volume/month increases.

The FDRS model implies a higher NW throughput requirement. Impact on Firewall and Intrusion Prevention Component.

The FRDS model implies a higher computing power requirement in the web and web application server layer.

The FRDS model implies less storage and backup storage capacity as less data is stored centrally.

The DB compute requirement is estimated to be higher in the SRDS model.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve a higher application operations, support & maintenance release testing workload

主要结论

在应用相关假设的情况下，与同步 RDS (SRDS) 模型相比，联合 RDS (FRDS) 模型中核心 RDS 系统的成本要略低一些。

FRDS 模型对于反向查询负载的变化情况高度敏感。反向查询的数量越大，FRDS 模型的成本会明显增加：反向查询负载为 3% 时，与 1% 的反向查询负载相比，FRDS 模型的成本预计会增加约 35%。这是与 FRDS 模型相关的一个重要的不确定风险因素。相反，人们认为 SRDS 模型对于反向查询的数量不太敏感。

FDRS 模型将需要更高的应用程序操作、支持、维护和测试成本，因为预计它会与注册管理执行机构进行更多交互。

此外，FRDS 模型对注册管理执行机构的影响也更大。在 FRDS 模型中，每个注册管理执行机构必须为在线查询提供支持（根据 SLA），这包括反向查询和历史所有权查询（亦称 WhoWas）。对于后者，注册管理执行机构必须为其维护历史数据。

附录 G：EPP 和 RDAP 协议支持 RDS 的能力

数据元素	EPP 是否支持收集	RDAP 是否支持访问
域名	是	是
注册状态	是	是
DNS 服务器	是	是
DNSSEC 授权	是	是
客户端状态	是	是
服务器状态	是	是
注册服务商	是	是
分销商	是	是
注册服务商所在辖区	否	否
注册管理机构所在辖区	否	否
注册协议语言	否	是
创建日期	是	是
原始注册日期	是	是
注册服务商到期日期	是	是
注册人类型	否	是*
PBC 名称	是	是
PBC ID	是	是
PBC 验证状态	否	否
PBC 上次验证时间戳	否	否
PBC 所在组织	是	是
PBC 街道地址	是	是
PBC 所在城市	是	是
PBC 所在州/省	是	是
PBC 邮编	是	是
PBC 所在国家/地区	是	是
PBC 电子邮件地址	是	是
PBC 备用电子邮件地址	否	是
PBC 电话 + 分机	是	是
PBC 备用电话 + 分机	否	是
PBC 传真 + 分机	是	是
PBC 短信号码	否	是
PBC 即时通讯地址	否	是
PBC 社交媒体、备用 SM	否	是
PBC 联系人和滥用问题 URL	否	是

数据元素	EPP 是否支持收集	RDAP 是否支持访问
更新日期	是	是
注册人姓名	是	是
注册人联系人 ID	是	是
注册人联系人验证状态	否	否
注册人联系人上次验证时间戳	否	否
注册人组织	是	是
注册人公司标识符	是	是
注册人街道地址	是	是
注册人所在城市	是	是
注册人所在州/省	是	是
注册人邮编	是	是
注册人所在国家/地区	是	是
注册人电话 + 分机	是	是
注册人传真 + 分机	是	是
注册人电子邮件、备用电子邮件地址	是	是
注册人 SMS	否	是
注册人 IM	否	是
注册人社交媒体、备用 SM	否	是
注册人联系人和滥用问题 URL	否	是
注册服务商 URL	否	是
注册服务商 IANA 号码	否	是*
注册服务商滥用问题联系人 电子邮件地址	否	是
注册服务商滥用问题联系人 电话号码	否	是
Internic 投诉站点 URL	否	是

* RDAP 中未明确指定这些数据元素。可以使用“remarks”（备注）字段或协议扩展返回这些元素。

协议扩展和/或附加

注册服务商和注册管理机构管辖区：需要将其添加到 EPP 或从当前的注册服务商位置信息中推导。可以使用 RDAP 实体“remarks”（备注）或通过协议扩展返回。

注册协议语言：需要通过协议扩展将其添加到 EPP。

注册人类型：需要通过协议扩展将其添加到 EPP。

注册人/PBC 验证状态、上次验证时间戳、备用电子邮件、备用电话 + 分机、SMS、IM、社交媒体、备用社交媒体、联系人 URL、滥用问题 URL：需要通过协议扩展将其添加到 EPP。RDAP 可以处理社交媒体标识符，但需要制定规范来定义此类标识符的格式。

联系人类型：当前可用的类型为“管理”、“付款”和“技术”。其他联系人类型将需要扩展 RDAP

RDAP 查询中指定的目的：需要通过协议扩展将其添加到 RDAP。

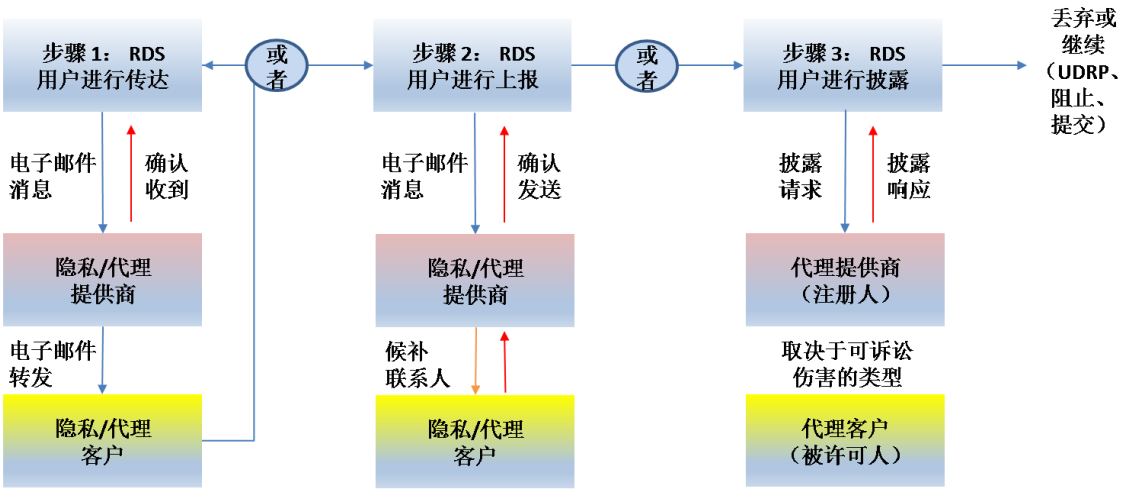
EPP 中的访问级别：EPP 包括了一个简单的机制，用于从注册服务商处收集注册人联系人元素披露首选项并将其传递给注册管理机构；通过该机制，可以将这些首选项用于告知 RDAP 响应行为。但是，该机制不够细化，无法在每个数据元素级别获取首选项。因此，将需要新的 EPP 扩展和/或联系人映射来指明注册人或联系人的选择，以覆盖每个数据元素的披露默认值（例如，默认情况下选择发布网关元素）。

附录 H：传达与披露模型和原则

如第 VI(b) 部分所述，EWG 建议通过委任的隐私和代理服务传达转发电子邮件地址收到的所有电子邮件。这样做的目的，是为可能希望联系他们的委任隐私/代理客户和 RDS 用户提供一个标准、始终可用且几乎实时的通信路径。

此外，EWG 还建议要求委任的代理服务及时响应披露请求（下文提供了详细说明）。这样做的目的，是为代理注册的域名出现严重问题的用户提供一个标准、始终可用的有效流程来寻求高效的问题解决办法。

分析这些用户需求时，EWG 注意到当前做法的另一个不足之处：在通信失败时，缺乏立即可用的高效上报方法。由于没有其他资源，许多用户快速跳到披露阶段。EWG 建议引入一个上报流程，对所有相关方来说，这样的成本可能更低，并且会减少导致更加昂贵和费时的披露请求的问题数量。这个三步流程如下所述：



步骤 1：传达

a) RDS 用户通过检索以下信息，请求某个域名的联系数据：

- 注册人的联系人 ID（即，隐私客户或代理服务提供商的联系人 ID）

- 所有必需的基于目的的联系人 (PBC) 的联系人 ID 和发布的 PBC 地址（包括电子邮件地址）

- 通过隐私/代理服务已完成域名注册的迹象，以及

- 委任的隐私或代理服务提供商（作为隐私/代理服务提供商 PCB 提供）的名称和地址，包括发布的传达上报和披露表单 URL。

b) RDS 用户注意到这是委任的隐私/代理注册，尝试通过转发地址向隐私/代理客户发送电子邮件。提供商可以选择让客户提供更多转发地址（如，电话、SMS、邮政地址）。

c) 必须要求委任的隐私/代理服务提供商转发并确认收到传达的消息（例如，通过电子邮件确认转发电子邮件地址收到的所有消息）。在出现错误的情况下（例如，无此类邮箱）可能会返回否定确认，并且可能会通过阈值来限制给同一发送者的确认，以防止传达滥用。

d) 收到确认的 RDS 用户现在已确认，消息被传达给了隐私/代理客户。但是客户可以选择不回复或者不阅读而丢弃传达的消息（例如，将其视为垃圾邮件）。

步骤 2：上报

RDS 用户对等待隐私/代理客户做出响应感到厌烦，因此决定通过以下方式上报以前尝试的联系人：

a) 访问在步骤 1 中确定的受委任隐私或代理服务的网站，并填写包含以下内容的上报表单：

- RDS 用户的身份（可能会重复使用 RDS 查询凭证）
- RDS 用户进行联系的原因（可能是定义的原因的下拉列表）
- 隐私/代理注册的域名
- 要传达给客户的已上传消息（可能已加密？）
- 第一次尝试传达的时间戳

b) 必须要求委任的隐私/代理服务提供商直接联系客户（可能使用 RDS 用户无法访问的联系信息和/或方法），并在 N*[42] 天内返回“送达确认”。这时，同样会在出现错误的情况下（例如，未通过身份验证的用户、超时）返回否定确认，而且可以记录提交次数并通过阈值来限制该次数以防止滥用。

c) 收到确认的 RDS 用户现在已记录表明消息被交付给隐私/代理客户的证据。客户仍然可以选择不做出回复，但上报必须有助于解决基本通信故障，而不需要进行披露。

[42] * 超时时间因通过验证的身份和为进行联系而指定的原因而异。例如，执法部门/OpSec 调查犯罪/滥用的时间为 1 天；品牌持有人调查 TM 侵权的时间为 7 天；互联网消费者尝试联系网上商家的时间为 7 天。

步骤3：披露（仅适用于代理注册的域名）

RDS 用户等待委任的代理客户（被许可人）做出响应超时，并通过以下方式确定问题严重到足到提起刑事或民事诉讼：

a) 访问在步骤 1 中确定的受委任代理服务提供商的网站或与该提供商通话或向其发送电子邮件，然后提交包含以下内容的披露请求：

- RDS 用户的身份
- RDS 用户进行联系的原因（严格限定为可控诉损害）
- 代理服务提供商注册的域名
- 损害的证明文件（商标注册信息、滥用指控）
- 尝试传达/上报的时间戳（上报的案例编号？）

b) 必须要求委任的代理服务提供商进行调查，并通过在 N*[43] 天内返回“披露响应”来采取适当的行动。可以记录披露请求，并将其限定为由具有相应资格的 RDS 用户指控的可控诉损害[44]以防止滥用。

c) 根据可用于评估案例的证明文件，委任的代理服务提供商可：

- 向客户发送通知并传输域名（即，中断代理服务）
- 在犯罪调查期间临时挂起域名
- 向用户披露从事非法活动的被许可人的身份/联系信息
- 拒绝披露 — 明确确认代理对进一步使用域名负责。

此时必须制定政策，以详细说明充分的证明文件的内容构成以及必须在什么时候通知被许可人。此外，还需要制定明确的政策，说明当地法律的影响以及要考虑的因素。当前所做的就是上面这些，而没有任何监督、政策指南或说明拒绝/忽略披露的后果。

---

[43] * 超时时间因请求者和为进行联系而指定的原因而异。对于时间紧迫的调查，执法部门可能会直接转至步骤 3（披露）。为防止其他人直接跳到步骤 3，步骤 2 的时间期限必须足够短，工作必须足够少。

[44] ** 任何请求披露的用户都必须证实他们属于（或代表）遭受可控诉损害的一方。例如，指控 TM 侵权的品牌持有人或其代理人可以证明他们自己的域名与代理注册的域名类似。在将用户类型与损害类型对应时需要深入考虑。请将 GoDaddy 的代理注册域名投诉表单选项列表作为示例。

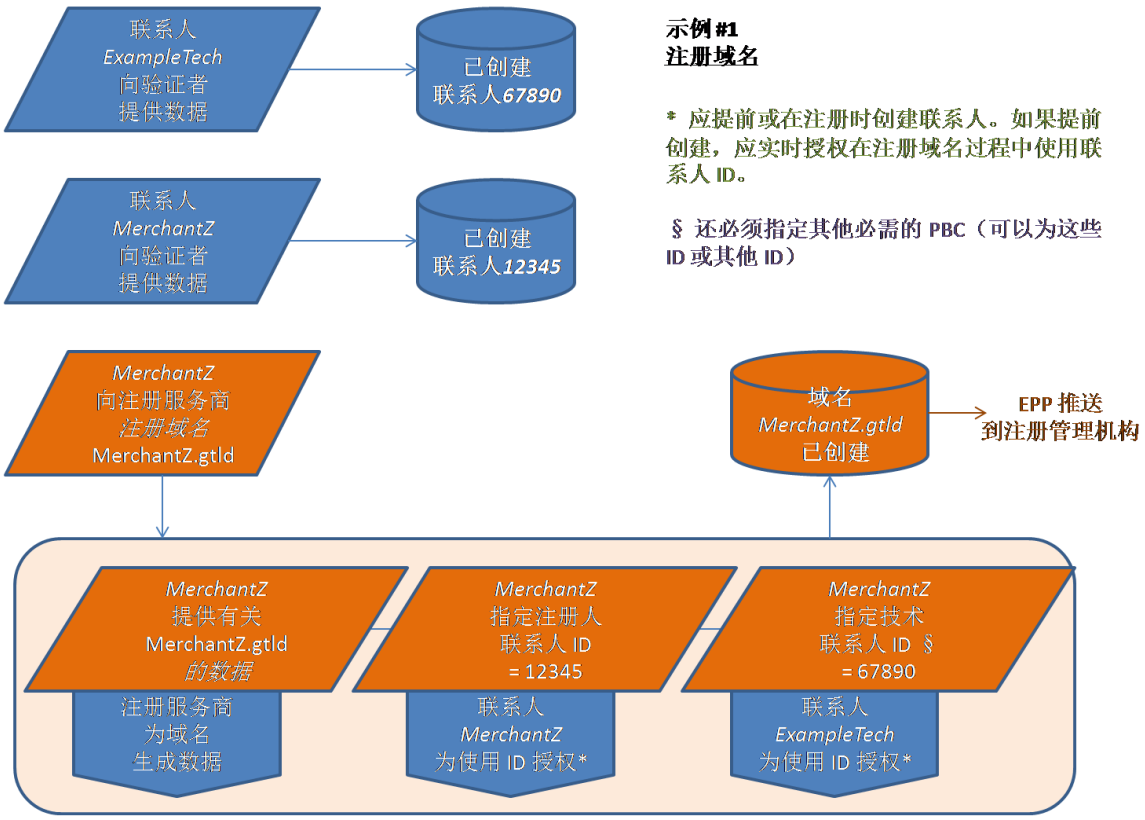
d) 收到披露响应的 RDS 用户现有具有结束该事件或提起法律/民事诉讼所需的信息。例如，商标侵权可能会导致提起 UDRP 投诉，而执法部门犯罪调查可能会导致嫌疑人被逮捕。如果披露被拒绝（或者未收到及时响应），RDS 用户现在还可以向委任的代理提起法律/民事诉讼。

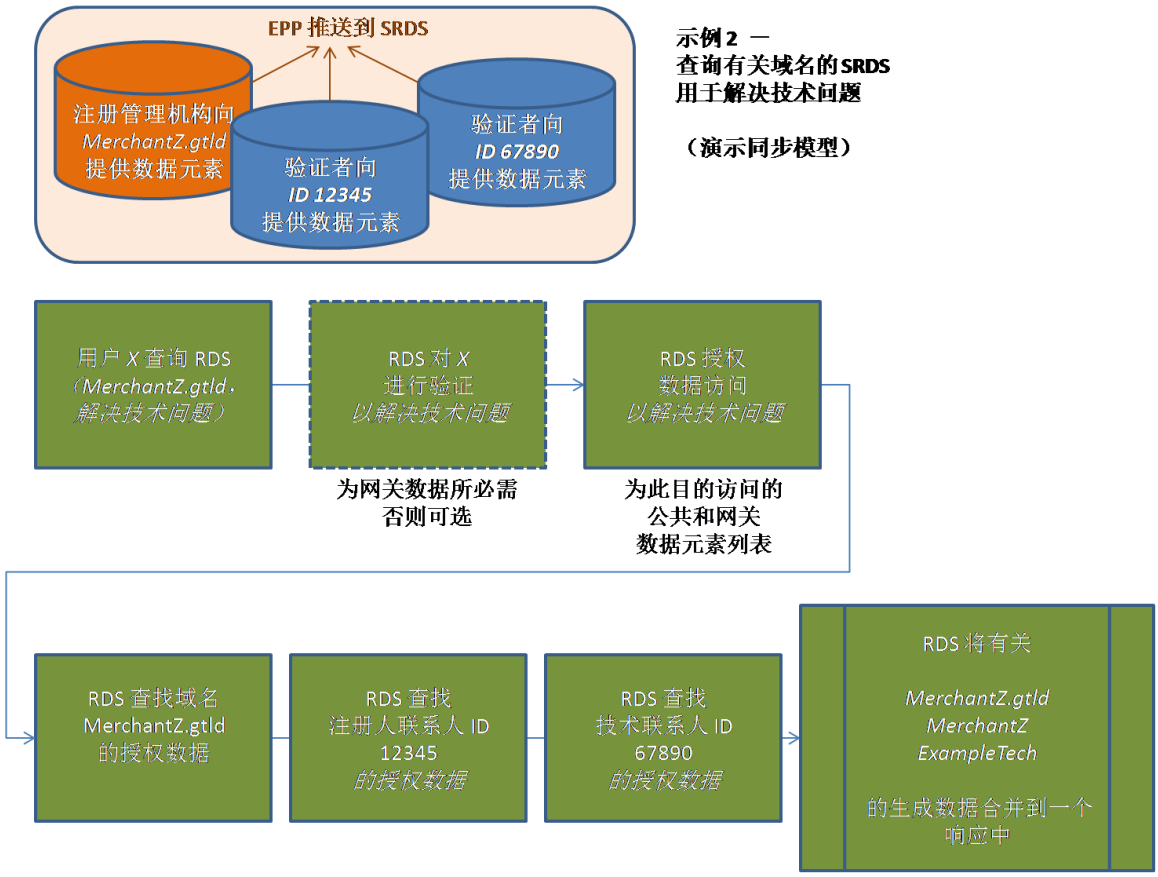
请注意，在代理或隐私注册必须向公众“曝光”而不只是向请求者“披露”时，上述流程无法解决问题。

GNSO PPSAI 工作组必须考虑 ICANN 机构群体的需求，并以 EWG 隐私和代理服务提供商在线调查的回应确定的最佳实践为参考，进一步优化这些建议的模型和流程。

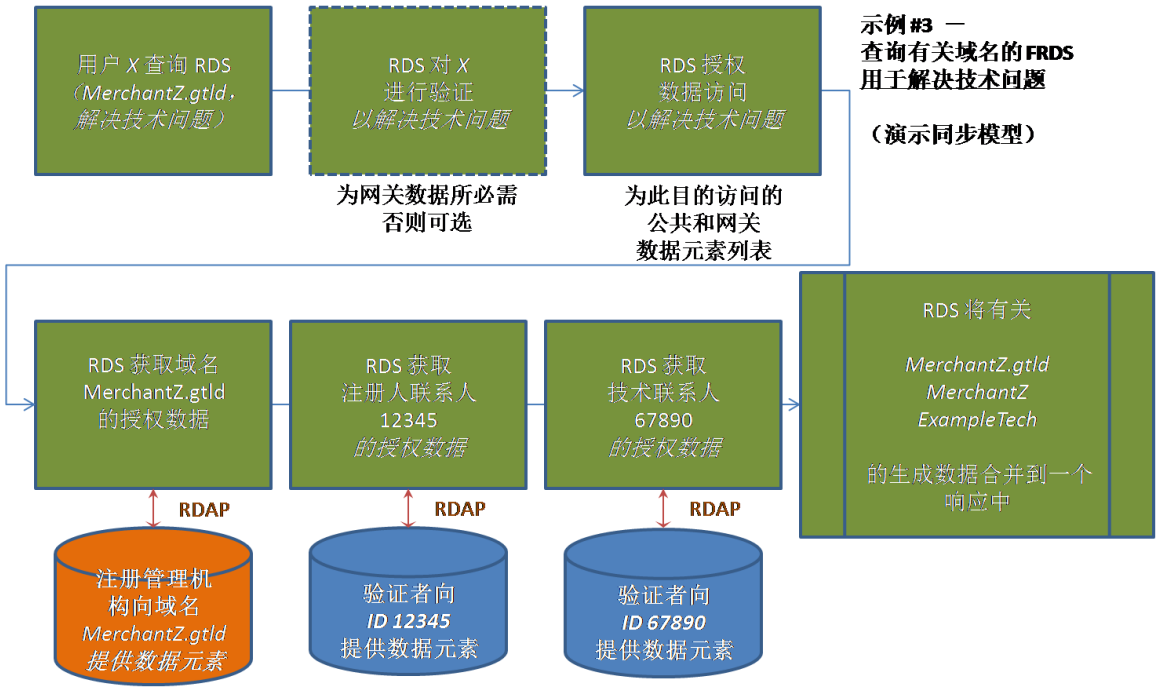
附录 I：RDS 流程图

以下流程图说明了域名注册期间以及请求者查询 RDS 以获取域名相关信息来解决技术问题时 RDS 生态系统参与者之间的关键数据流。





为便于进行模型比较，下面对 FRDS 重复使用了这同一个示例。



附录 J：关于 EWG

选举流程和愿景

在组建 EWG 时，ICANN 理事会采用了一个全新的方法来解决过去一直陷入僵局并且存在各种分歧的棘手问题。理事会将代表各种不同观点的个人和各个利益主体集中到一起，希望通过分享他们的专业技能成功解决其他方面未解决的问题。在工作组提交此最终报告及其 180 个基于共识的原则后，理事会的愿景已经得到真实体现。

EWG 的成员是在经验丰富且保持中立的推进者 Jean-Francois Baril 的帮助下精心推选出来的。选择 Jean-Francois 作为推进者是因为他在为消费电子行业制定标准方面拥有丰富的经验。筛选数十位 EWG 申请人的标准包括领导能力、专业技能、地理多样性、达成共识、创新能力以及中立性（在某些情况下）。各方认为，来自 ICANN 机构群体以外的个人能够带来全新的视角，不会由于过去尝试解决 WHOIS 问题而感到疲倦。

EWG 的构成

EWG 成员由来自澳大利亚、加拿大、中国、欧盟委员会、爱尔兰、牙买加、尼日利亚、挪威、瑞士、英国以及美国的个人、理事会联络员和工作人员组成。事实证明，这种地理多样性有助于了解与 EWG 工作关联的许多管辖区挑战。

EWG 成员包括经验丰富的企业家和全球领袖（Ajayi、Ala-Pietilä、Neylon、Rasmussen 和 Shah）。他们在平衡风险方面丰富的专业经验和注重实效的问题解决方式为在 EWG 内尽早达成共识奠定了基础。

由于 EWG 的使命包括考察公共政策，尤其是隐私问题，因此，政府部门方面的特定专业知识对于它的成功非常关键。Perrin 和 Niebel 拥有在加拿大和欧洲的工作经验，可确保在设计下一代系统时重点考虑这些问题。重要的是，在其进行磋商期间，EWG 应了解并设法关注欧盟数据保护立法的最新动态。

EWG 工作的另一个重要方面是确保可在当前 DNS 生态系统内适当实施它的建议。gTLD 注册服务商 (Neylon)、gTLD 注册管理机构（Hollenbeck-.com 和 .net）以及 ccTLD（.cn-Jian、.uk-Nanayakkara、.ng-Ajayi 和 .au-Disspain）成员拥有的专业知识可为解决验证方法、隐私/代理注册、与 EPP 和 IETF 正在开发的新 RDAP 等协议兼容，以及合并“网关访问”之类的概念来显示敏感数据元素等问题提供启示。

此外，还利用现任和往届 SSAC 成员（Crocker 和 Rasmussen）的洞察力及其对执法部门在打击有关 DNS 的恶意滥用方面的深入了解，针对安全性和稳定性问题进行了分析。

如果不考虑许多用户对下一代 RDS 的要求，将无法设计新的系统。EWG 中的一些成员（Kawaguchi、Vayra 和 Shah）对知识产权问题具有深入的了解，他们在很大程度上依赖当前的 WHOIS 系统来打域名恶意抢注、欺诈和在线仿冒；同时，最终用户（Samuels 和 Phifer）也分享了他们的观点。这些不同的视角有助于确保通过 RDS 合法访问注册数据，同时尽可能最大限度地减少当前注册流程中的低效现象和滥用情况。

为了加强 EWG 的力量，ICANN 工作人员（Michel、Milam）还提供了执行启示和 ICANN 合同框架方面的知识。此外，一名顾问 (Phifer) 还提供了过去五年中进行的详尽 GNSO WHOIS 研究所获得的数据，以帮助 EWG 根据事实提出建议。

工作方法

EWG 通过一系列相互了解活动来开展其工作；这些活动旨在促进和谐关系、培养互信，以及更重要的，建立团队归属意识。EWG 确定了一套团队价值观来克服为这个复杂的问题探求创新型解决办法时遇到的障碍。它们分别是：

- 作为团队中的一员
- 言论自由
- 无社交媒体归属
- 学术诚实
- 业界自律
- 全新设计
- 艰难现实中的因素（技术和政府）

这些价值帮助指导 EWG 在设计 RDS 以及提出本最终报告中阐述的原则时做出了必要的妥协。

有关详细信息及 EWG 成员的简历，请参阅本公告。