

下一代注册目录服务 专家工作组的 初步报告

本文档的来由状况

本文档是专家工作组 (EWG) 提交的报告，旨在为下一代 gTLD 注册目录服务（“RDS”）替代当前 WHOIS 系统提供建议。

II. EWG 的使命和目的	7
2.1 使命.....	7
2.2 指导 EWG 工作的目的声明	8
III. 方法 — 明确用户和目的	9
3.1 使用案例分析法	9
3.2 明确 RDS 的用户	10
3.3 明确需要满足或禁止的目的	14
3.4 RDS 中涉及的利益主体	15
3.5 共同需求	17
3.6 将数据元与可接受目的相对应.....	17
IV. 所需功能和设计原则.....	18
V. 建议的模式	24
5.1 多种系统设计的审查	25
5.2 建议的集中式 RDS	26
VI. 解决隐私权问题.....	28
VII. 网关访问功能说明	29
VIII. 结语和后续措施.....	31

I. 执行摘要

gTLD 目录服务专家工作组 (EWG) 是由 ICANN 首席执行官 Fadi Chehadé 应 ICANN 理事会的要求而组建的，旨在帮助打破 ICANN 机构群体内部持续了近十年之久的僵局，即如何替代当前被广泛认为“已被破坏的”WHOIS 系统。EWG 的使命是重新审查和定义收集和维护 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，探索和质疑关于注册数据的用途、使用、收集、维护和提供的基本假设，以及准确性、访问权、隐私要求和 gTLD 目录服务所涉及的利益主体。在研究了各种使用案例及其呈现的诸多问题后，EWG 得出结论：应当舍弃授予每个用户相同的匿名公共访问权（经常不准确）来访问 gTLD 注册数据的当前 WHOIS 模式。此外，EWG 建议改变模式，使 gTLD 注册数据的收集、验证和披露仅用于容许目的，而且只有通过身份验证的请求者才能访问某些数据元并负责进行合理使用。

EWG 建议的容许目的包括：

- 域名控制
- 域名研究
- 个人数据保护
- 法律诉讼
- 解决技术问题
- 监管/合同实施
- 域名购买/销售
- 个人互联网使用
- 减少滥用
- 提供互联网服务

EWG 考虑到收集、存储、披露和使用 gTLD 注册数据所涉及的利益主体的广度，将其与相关目的对应起来。然后，EWG 在制定原则和特性以便为下一代注册数据服务 (RDS) 的设计工作提供指导时，确定和考虑了共同需求方面的内容。

因此，EWG 对多个系统设计进行了考量，并就出于各种目的而收集、使用和披露准确的个人数据元的新注册数据服务模式达成一致意见。RDS 生态系统中的各方都具有不同的数据需求、面临着不同的风险以及可能承担着不同的责任。过去，大多数责任都转移给了以向付费客户提供有效域名为首要目标的注册服务商。随着互联网生态系统变得愈加复杂，以及数百个新 gTLD 的涌现，新的参与者可能需要承担一些责任，以满足如此广泛的注册目的。

下图说明了 EWG 建议的下一代 RDS 模式，其中可能包含本报告中讨论的很多原则。本集中式 RDS (ARDS) 模式的关键要素包括：

- ARDS 充当集中式存储库，其中包含收集的所有数据元的非权威副本
- 每个 gTLD 注册管理机构仍然是数据的权威来源
- 请求者（希望从系统中获得 gTLD 注册数据的用户）申请 ARDS 的访问凭证
- 解除注册服务商/注册管理机构提供端口 43 访问或其他公共访问要求的义务
- 在大多数情况下，ARDS 提供对缓存注册数据的访问，该数据复制自 gTLD 注册管理机构，并通过频繁的定期更新进行维护
- ARDS 也可以提供对实时注册数据的访问，该数据根据需要从 gTLD 注册管理机构实时获取，并受到控制以防止过度使用或滥用这一方案
- ARDS（或与 ARDS 交互的其他第三方）负责执行验证服务
- ARDS 负责审核访问，以最大程度减少滥用，并对不当访问给予处罚或采取其他补救措施
- ARDS 处理数据准确性投诉
- ARDS 管理数据访问的许可协定

ICANN 与国际第三方供应商签订合同，制定和运营 ARDS，并监控是否符合要求

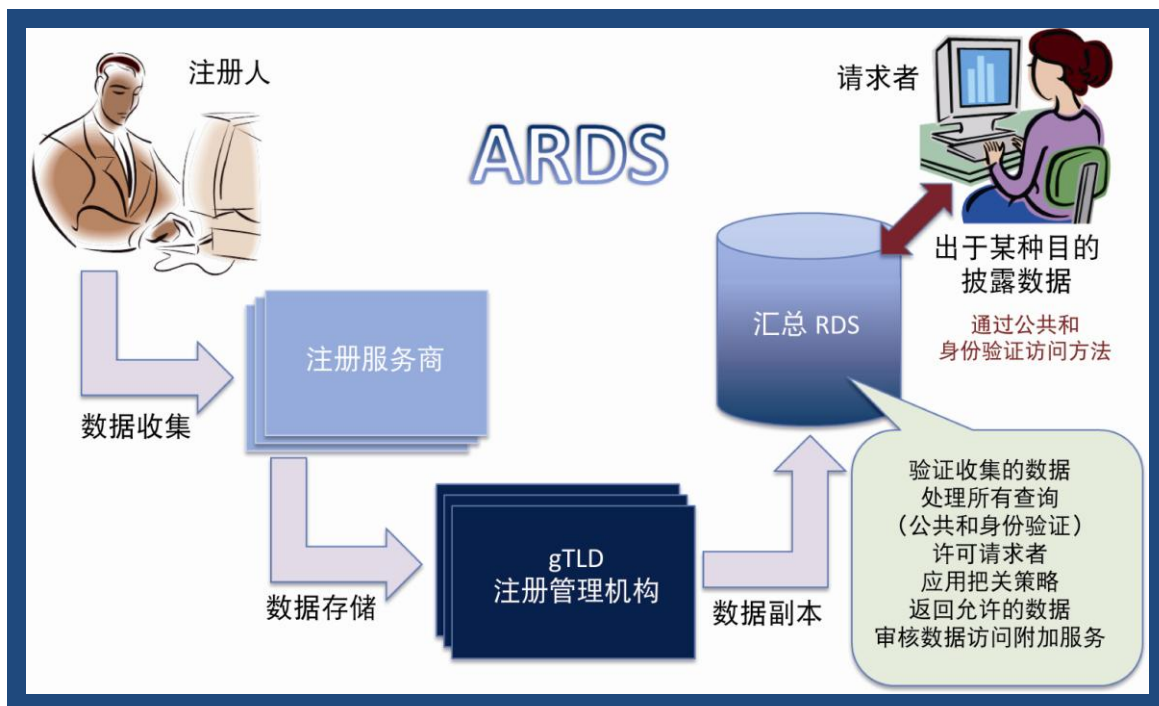


图 4. 集中式 RDS 模式

该模式拥有众多优点，获得了 EWG 成员的一致同意：

- 通过单一联系点来处理调整工作
- 在传输和递送方面可获得改进
- 为注册数据请求者提供“一站式”服务
- 加强了注册数据验证和访问的问责制（防止滥用）
- 能够以相同的方式在多个 TLD 之间跟踪/审核/惩罚请求者（防止滥用）
- 可减少注册服务商和注册管理机构当前因提供数据访问而承担的部分成本
- 可提供数据标准化或过滤功能
- 减小了注册服务商和注册管理机构的带宽要求
- 有助于使方法标准化，以解决本地数据隐私权问题
- 提高了跨多个 TLD 的搜索能力（例如反向查询）
- 最大程度地减少了过渡和实施成本
- 能够验证/认可具有特殊目的（如执法）的请求者
- 有助于更有效地管理不准确的报告
- 能够进行更有效的随机准确性检查
- 能够以多种语言、脚本和字符显示用户友好的搜索门户网站

当然，金无足赤。EWG 同时也考虑了该模式可能存在的缺点：

- 数据延迟
- 创建了包含极高价值数据的“大数据”源，如果审核和维护不当，可能造成滥用
- 增加了内部人员滥用和外部攻击的风险，需要更加重视安全策略的实施、执行和审核
- 注册管理机构/注册服务商不再控制注册数据的交付

在提出这一新模式时，EWG 意识到了准确性需求，以及保护可能要求加强个人信息保护的注册人的隐私的需求。EWG 已讨论了 RDS 可用于满足风险用户需求的方法，即使用“安全保护凭证”来最大程度地保护注册服务。其中一个方案是，可以使用一套议定标准，让 ICANN 委任一个独立的组织来充当“受信任的代理机构”，由该机构确定注册人是否有资格获得最大保护。EWG 期望深入思考安全保

护凭证的潜在模式，这可能有助于在问责制和风险互联网用户的个人数据隐私需求之间找到极具创新性的有效平衡。

后续步骤

尽管这些建议中反映出了所取得的进展，但 **EWG** 尚未完成其审议工作。工作组会就这些建议草案征询公众意见，并将在仔细考虑在 **ICANN** 德班会议和其他公众意见征询期间通过在线方式收到的意见后，继续修订其建议。

此外，还有几个关键问题有待充分研究，例如：

- 将强制性/可选数据元与每个目的对应起来
- 确定需要进行风险和影响分析的领域
- 考虑成本和影响，以及承担成本和影响的方法
- 研究多模式访问方法，以及如何通过现有或未来的注册数据访问协议来启用这些方法

在针对本初步报告征询公众意见后，**EWG** 将发布最终报告并将其提交给 **ICANN** 首席执行官和理事会，以在适当时作为新 **gTLD** 政策和合同谈判的基础。如理事会所称，基于最终报告的问题报告将构成理事会发起的、受到密切关注的 **GNSO** 政策制定流程 (**PDP**) 的基础。

II. EWG 的使命和目的

2.1 使命

EWG 的成立是履行 ICANN 理事会指令¹的第一步，旨在帮助重新定义 gTLD 注册数据（例如 WHOIS）的用途和提供规定，同时达到为 gTLD 目录服务和合同协商制定新的全球政策提供基础的既定目标。EWG 的目标包括：1) 定义收集和维护 gTLD 注册数据的目的，并考虑如何保护这些数据，以及 2) 为管理 gTLD 目录服务提供拟议模型，以解决相关的数据准确性和访问问题，同时考虑用于保护数据的保障措施。EWG 参考了 [WHOIS 审查小组最终报告](#)、[GAC WHOIS 原则](#)，以及先前的机构群体意见和 GNSO 在过去十年的工作。此外，EWG 还按照要求处理了安全与稳定咨询委员会 (SSAC) 在 [SAC055](#) 报告中提出的关键问题、考量了当前和将来的互联网运作及服务，并在 ICANN 的事务处理范围内评估了提供、收集、维护、发布或使用此类数据的各方的问题。

¹理事会决议发布地址：<http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm>。

附录 A 强调了 EWG 对理事会提出的具体问题的回应。

2.2 指导 EWG 工作的目的声明

为了帮助指导 EWG 的审议工作，工作组发表了一份高级目的声明，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性
- 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

III. 方法 — 明确用户和目的

3.1 使用案例分析法

在定义下一代注册目录服务的工作中，EWG 尽量从零开始，而不是在当前 WHOIS 系统的基础上进行改进，这一方法被广泛认为不足以解决问题。按照理事会的指令，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。

为了实现这一目标，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 B](#) 查看 EWG 考量的使用案例清单。

为了确定 RDS 应涵盖的各类利益主体和所需目的，以及系统应试图阻止的一系列潜在滥用行为（将在本报告后续章节详细讨论），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，研究了下面图 1 中所示的各个领域的具体需求。

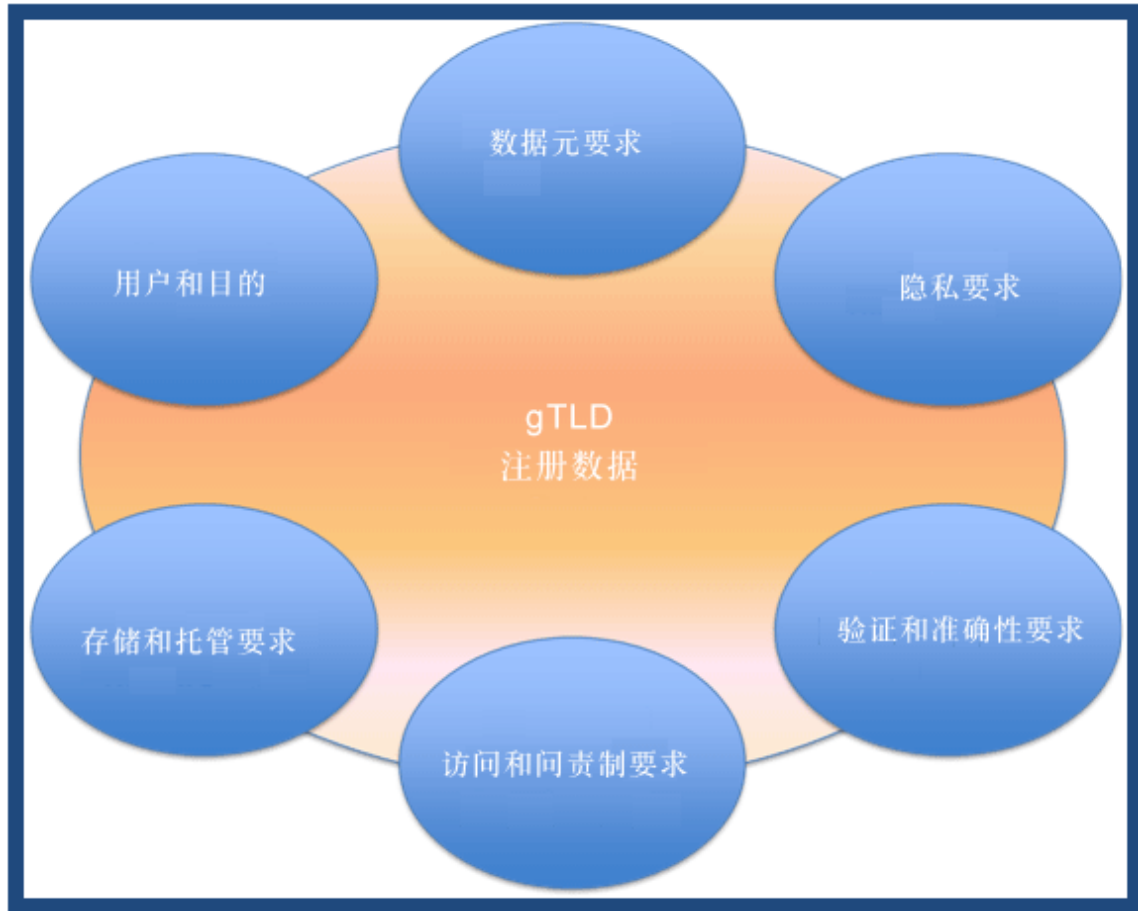


图 1：需求分析

EWG 预计会继续分析这些目的和需求，以确定最小数据元、相关风险、隐私法律和政策含义，并在本报告的最终草案中对更多问题进行更加充分地探讨。

3.2 明确 RDS 的用户

EWG 分析了每个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。有关每个使用案例以及用户与 RDS 之间的交互的更多详细信息，请参见[附录 B](#)。

用户	目的	使用案例	访问注册数据的理由
所有注册人 (如自然人、法人、隐私/代理服务提供者)	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创建新的注册服务商帐户来注册域名
		域名 数据修改监测	检测域名注册数据是否遭到意外、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	使注册人能够发起对另一注册服务商的域名迁移
		域名 删除	能删除过期域名
		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	使域名的付款联系人(个人、职能角色或实体)能够续用已注册的域名
		域名 联系信息验证	便于对域名注册数据(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 (如隐私/代理服务的客户)	个人数据 保护	加强注册保护	使任何希望最大程度减少对个人姓名及地址进行公共访问的注册人都能使用经认可的隐私或代理注册服务
		最大程度保护注册	使受到威胁的个人或群体能够利用可信第三方颁发的不具名凭证来使用经认可的代理注册服务
互联网技术人员 (如管理员、邮件管理员、网络管理员)	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)
在线服务提供商 (如 ISP、托管服务提供商、CA、声誉服务提供商)	提供互联网 服务	联系域名注册人	当提供商无法使用常用联系方法联系客户(个人、职能角色或实体)时,能重新建立与客户之间的联系以处理有关域名的业务问题
		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
		域名认证服务	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	为消费者提供一种低调机制,便于消费者在没有 LE/OpSec 干预的情况下联系域名注册人(如网上零售商),从而快速解决问题
		法律/民事诉讼	帮助受害者个人识别涉嫌参与非法活动的域名注册人,进而使 LE/OpSec

用户	目的	使用案例	访问注册数据的理由
			能进一步展开调查
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	通过经纪人的域名销售	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(如有)
		域名注册历史	提供域名注册历史以确定过去的注册人和日期
		指定注册人注册的域名	能确定由指定实体注册的所有域名(如合并/分派资产核查)
互联网研究员	域名研究	域名注册历史	研究和统计分析域名注册相关事宜(互联网企业用户也需要这样做)
		指定注册人注册的域名	研究和统计分析域名注册人(互联网企业用户也需要这样做)
		域名注册人联系信息	能调查域名注册人(在线服务提供商也需要这样做)
知识产权所有人 (如品牌持有人、商标所有者、知识产权所有人)	法律诉讼	代理服务提供商客户鉴定	针对可能因涉嫌侵权或知识产权盗窃而正在遭受调查的域名,能够鉴定与该域名有关的代理服务的客户身份(即披露身份)
		域名用户联系信息	针对因 TM/品牌侵权或知识产权盗窃而正在遭受调查的域名,能够与使用该域名的当事方联系
		打击对注册数据的欺诈性使用行为	便于识别对属于另一注册人的合法数据(如地址)的欺诈性使用并作出响应
非 LEA 调查员 (如税务机构人员、UDRP 提供商、ICANN 合规工作人员)	监管和合同实施	网上税务调查	便于国家、州、省或当地税务机关对网上销售的域名进行鉴定
		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
		RAA 合同合规性	让 ICANN 合同合规性部门负责审核和答复有关注册服务商行为的投诉(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)	减少滥用	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
		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指定的滥用问题处理人员/ISP 以协助修复受攻击域名

用户	目的	使用案例	访问注册数据的理由
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. 用户

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，以及与其相关的利益主体和数据。



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。正如下文第 IV 节详细讨论的那样，EWG 建议舍弃授予每个用户相同的匿名公共访问权（经常不准确）来访问 gTLD 注册数据的当前 WHOIS 模式（以及协议）。此外，EWG 建议改变模式，使 gTLD 注册数据的收集、验证和披露仅用于容许目的，而且只有通过身份验证的请求者才能访问某些数据元并负责进行合理使用。

3.3 明确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 曾试图给第 3.2 节所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。正因为如此，EWG 建议，除了应该受到积极阻止的已知恶意互联网活动以外，对于第 3.2 节中提到的所有目的，RDS 都应以某种方式给予满足。EWG 建议容许目的如下图所示。



图 3：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 在成立时应被赋予容纳这些新用户和容许目的的职能。

3.4 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。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（如注册服务商、注册管理机构）或披露数据（如 RDS 运营商、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（如域名滥用问题联系人）。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指定交易中，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
域名滥用问题联系人	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/合同实施
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	提供互联网服务
投诉人	监管/合同实施
使用网站的用户	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/合同实施
ICANN 合规工作人员	监管/合同实施
互联网服务提供商	减少滥用
调查员	个人互联网使用
执法人员	减少滥用 法律诉讼
列明的联系人	提供互联网服务
在线服务提供商	提供互联网服务
Op/Sec 服务提供商	减少滥用

赞助研究的机构	域名研究
受到调查的个人/实体	监管/合同实施
隐私/代理服务客户	企业域名的购买或销售 域名控制 提供互联网服务 监管/合同实施 个人数据保护
隐私/代理服务提供商	减少滥用 企业域名的购买或销售 域名控制 域名研究 提供互联网服务 法律诉讼 个人数据保护 监管/合同实施 解决技术问题
RDS 运营商	所有目的
注册人	所有目的
注册人的代理人	企业域名的购买或销售 提供互联网服务 监管/合同实施
注册服务商	企业域名的购买或销售 域名控制 域名研究 个人互联网使用 提供互联网服务 法律诉讼 个人数据保护 监管/合同实施 解决技术问题 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	域名研究
分销商	减少滥用
问题解决者	解决技术问题
法律/民事诉讼的对象	个人互联网使用
技术联系人	解决技术问题
寻求联系的第三方	法律诉讼 个人数据保护
受信任的代理机构	个人数据保护
UDRP 专家小组成员	监管/合同实施
UDRP 提供商	监管/合同实施
需要加强保护的验证者	个人数据保护
滥用受害者	减少滥用
Web 托管服务提供商	解决技术问题

表 2. 代表性利益主体一览表

3.5 共同需求

在分析了众多使用案例之后，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

不过，也有一些需求虽然是许多用户共同的需求，但当前 WHOIS 系统却并未始终如一地加以满足。例如：

- 用以确定被某一已知实体注册的所有域名
- 用以确定域名首次注册的时间

针对这一方面，EWG 在制定用以指导 RDS 设计的建议原则时，将这些共同需求一并纳入了考虑范围。不过，由于后面不断会有其他共同需求涌现，因此设计时应牢记系统设计必须具有可扩展性。

3.6 将数据元与可接受目的相对应

[附录 C](#) 给出了与每个可接受目相关的数据元。在这些数据元中，某些应收集起来供每个域名使用，而其他则可选择性地收集供某一组域名使用。另外，对于已收集的数据元，既可让请求者通过 RDS 访问，也可不让请求者访问。未来，EWG 预计会进一步考虑这些问题，从而得出有关这方面的初步建议，不过就目前而言，EWG 建议应对所有数据元进行更为彻底的风险和影响分析，从而完成分类。对于要如何执行这一风险和影响分析、应该由谁执行以及判定各个数据元是否必须通过公共或网关访问方式进行收集和披露应该依据什么标准这几个方面，EWG 认为公众的意见应该会有所帮助。

IV. 所需功能和设计原则

鉴于将来会在许多领域内执行适当的风险和影响分析，EWG 认为，下一代注册目录服务 (RDS) 应包括以下功能和设计原则：

	功能	EWG 设计原则
4.1	适用性	
	4.1.1	<ul style="list-style-type: none"> • RDS 必须适用于所有现有的或新增的 gTLD 注册管理机构。不允许任何追溯或特别豁免。
4.2	国际因素	
	4.2.1	<ul style="list-style-type: none"> • 每个参与 RDS 的利益主体都应针对数据访问、数据使用、数据保留和正当流程制定一项或多项政策。 <ul style="list-style-type: none"> ○ 管辖区不同，政策也可能会有所不同。 ○ 这些政策必须遵守当地法律。 ○ EWG 预计会进一步探讨这些问题。
	4.2.2	<ul style="list-style-type: none"> • 为实现真正的全球化，RDS 应能以多种语言、脚本和字符集显示注册数据 <ul style="list-style-type: none"> ○ IDN 专家有必要进行额外的分析以明确这些要求。
4.3	问责制	
	4.3.1	<ul style="list-style-type: none"> • 域名生态系统中的各方都对彼此负有责任。
	4.3.2	<ul style="list-style-type: none"> • 注册人负责及时地向 RDS 中提供当前的准确注册数据并对这些数据加以维护。
	4.3.3	<ul style="list-style-type: none"> • 当域名出现任何问题时，注册人负责确保能联系到相关人士以便及时解决问题。
	4.3.4	<ul style="list-style-type: none"> • 在域名的注册和使用方面，注册人应承担全部责任。
	4.3.5	<ul style="list-style-type: none"> • 注册服务商负责依据合同规定向注册人提供服务，包括确保提供当前的准确注册数据。
	4.3.6	<ul style="list-style-type: none"> • 若提供和维护的数据不准确，应承担一定的后果。

		<ul style="list-style-type: none"> ○ EWG 预计会进一步探讨这一问题。
4.4	隐私因素	
	4.4.1	<ul style="list-style-type: none"> ● RDS 应满足人们关于隐私保护的需求，包括： <ul style="list-style-type: none"> ○ 满足一般个人数据隐私需求的加强保护注册服务；以及 ○ 为存在风险且言论自由的用途提供安全保护凭证服务的最大保护注册服务。 ● 应对隐私/代理服务提供商进行委任并针对提供和使用经认可的隐私/代理服务制定相应的规则。 ● 除了利用经认证的隐私/代理服务而注册的域名以外，所有注册人都应对他们所注册的域名承担责任。 ● EWG 预计会进一步探讨这一问题，包括： <ul style="list-style-type: none"> ○ 所有经委任的隐私和代理服务提供商要实施的标准化流程。 ○ 经委任的执法机构制定的特殊请求处理流程。 ○ 获得许可的其他许可者（如知识产权所有人）制定的特殊请求处理流程。
	4.4.2	
	4.4.3	
	4.4.4	
4.5	容许目的	
	4.5.1	<ul style="list-style-type: none"> ● 应明确规定系统的容许/不容许目的。 ● 第 3 节大致说明了 EWG 规定的可接受用途。
	4.5.2	
4.6	数据披露	
	4.6.1	<ul style="list-style-type: none"> ● RDS 应提供出于某种目的的数据元披露。 ● 并非所有收集的数据都可向公众披露；是否披露取决于请求者及其使用目的。 ● 应允许对经确认的最小数据集的公共访问，但限制批量获取。 ● 对于在风险和影响评估后确定为较敏感的数据元，应通过网关访问加以保护，只有在以下情况下才允许披露： <ul style="list-style-type: none"> ▪ 确认属于容许目的 ▪ 如实披露请求者/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 ● 对于一些在风险和影响分析后确定为
	4.6.2	
	4.6.3	
	4.6.4	
	4.6.5	

	4.6.6 4.6.7	<p>极其敏感的数据元，可通过规定的法律流程（如传唤）进行访问。</p> <ul style="list-style-type: none"> 只能披露允许用于宣称目的的数据元。 附录 C 针对附录 B 中的具体可接受用途给出了对应的数据元。
4.7	数据元	
	4.7.1 4.7.2 4.7.3 4.7.4 4.7.5	<ul style="list-style-type: none"> 所有收集的数据元都必须至少具有一个容许目的。 所有数据元都应根据确定的可接受用途与容许目的对应起来。 待收集、存储和公开披露的最小数据源的确定应基于风险评估。 为了实现可扩展性，对于注册管理机构收集的所有其他数据元，系统应允许通过常见的访问方式和接口进行访问，从而将其纳入系统中。 完整的数据元集应由注册管理机构存储。
4.8	访问方式	
	4.8.1 4.8.2 4.8.3	<ul style="list-style-type: none"> 所有访问应遵循无歧视原则（即，访问流程应为所有出于同一目的的请求者创建一个公平竞争的环境）。 为了防止滥用并推进问责制， <ul style="list-style-type: none"> 所有访问都应经过验证以确保符合适当的级别；以及 要求访问数据元的请求者应能够申请并获得后续验证数据访问查询时需要使用的凭证。 应对网关访问请求者实施某种类型的认证 <ul style="list-style-type: none"> 当经认证的请求者查询数据时，其目的应 <ul style="list-style-type: none"> [选项 a] 为默认，还是 [选项 b] 在每次发送请求时陈述一遍？² 对于不同目的应制定不同的条款和条件。

² EWG 预计会进一步探讨这两个选项。

	<p>4.8.4</p> <p>4.8.5</p> <p>4.8.6</p> <p>4.8.7</p>	<ul style="list-style-type: none"> ○ 一旦违反了这些条款和条件，经认证的请求者应受到相应处罚。 ● 所有查询/响应都应保护传输数据的机密性和完整性。 ● 可提供付费数据访问服务（如逆向WHOIS、WhoWas），但需建立某种类型的认证制度。 ● 所有数据披露都应通过规定的访问方式进行。不得通过未受控制的访问批量导出完整数据集。 ● 披露包括显示和其他输出方式。 <ul style="list-style-type: none"> ○ 为了能始终如一地轻松找到数据和访问数据，应建立一个访问中心（如门户网站）。 ○ 使所有请求者都能通过匿名查询的方式访问公共数据（以最小程度，通过网站）。 ○ 对于符合要求的请求者和使用目的，允许请求者通过网络和其他访问方式及格式（如xml响应、SMS、电子邮件）对敏感数据进行网关访问。 ○ 使请求者能在有需要时实时获得权威数据。
<p>4.9</p>	<p>验证和准确性</p>	
	<p>4.9.1</p> <p>4.9.2</p> <p>4.9.3</p>	<ul style="list-style-type: none"> ● 为了提高数据质量，应在收集注册数据时对其进行句法验证（即，检查格式是否正确 [依据 SAC58]）。 ● 为了提高数据的可用性，应对注册人姓名/联系方式数据进行操作验证（即，检查利用这些数据是否可联系到注册人）。 ● 为了减少欺诈行为 <ul style="list-style-type: none"> ○ 在注册人首次注册域名前，应通过提供全球唯一的注册人姓名/组织及相应的联系方式对注册人进行预验证。 ○ 经过预验证确认数据准确无误且具有唯一性后，应向该注册人发

	<p>4.9.4</p> <p>4.9.5</p> <p>4.9.6</p> <p>4.9.7</p> <p>4.9.8</p> <p>4.9.9</p> <p>4.9.10</p>	<p>放授权代码（如 PIN）。在没有此授权代码的情况下，同一³名称/组织不得注册多个域名。</p> <ul style="list-style-type: none"> ○ ICANN 应与第三方提供商签订合同，委托该方负责提供预验证服务和发放授权代码。 <ul style="list-style-type: none"> ● 为了改善数据的一致性和统一性并简化维护工作， <ul style="list-style-type: none"> ○ 经过预验证的数据元应能够重复使用，即用于将来的域名注册，可根据每个域名重新设置这些默认数据。 ○ 预验证数据元的任何更新都可自动应用到所有链接域名。 ● 为了提高数据质量，对于那些未经预验证的注册人姓名/联系方式数据，仍应进行某种方式的验证（如通过带有姓名/联系方式的信用卡成功支付来暗中确认）。 ● 为了在保证质量的同时保持快速激活，延迟验证注册人姓名/联系方式不得阻止域名成功注册和载入 DNS 清单。不过，若在规定期限内仍未进行验证，则这类域名可能会被标记并暂停/删除。 ● 为了从全球各地成功验证注册人的姓名/联系方式，采用操作验证方法时不能只验证一个联系方式（如邮政地址）。 ● 为了在以后仍能保持数据的高质量，经过验证的数据元应定期进行重新验证，例如，更新注册人姓名/联系方式时或转移域名与之前验证的姓名/联系方式的链接时。 ● 系统应明确记录每个数据元是否经过验证以及验证时间，即使对从未披露过的数据元也不例外。 ● 为了帮助拥有高质量姓名/联系方式数据的注册人成功注册域名，注册人必须了解注册流程及其相关的政策。
<p>4.10.</p>	<p>标准验证服务</p>	

³ EWG 预计会进一步探讨该问题。

	4.10.1 4.10.2	<ul style="list-style-type: none"> • 使用标准验证服务是最佳选择，这是因为它： <ul style="list-style-type: none"> ○ 降低了注册服务商/注册管理机构的成本并减少其负担。 ○ 能更高效地给验证数据库授权，如UPS 地址复核比对、黄页、企业/公司、政府注册管理机构、选民名册、信用局记录等。 ○ 适当实现了特定国家/司法管辖区的验证流程的标准化。 ○ 减少了有关注册管理机构/注册服务商的合规性查询的数量。 • ICANN 应与提供标准验证服务的第三方提供商签订合同以确保注册数据准确性合规、通过审核且可用。
4.11	合同关系	
	4.11.1 4.11.2 4.11.3 4.11.4	<ul style="list-style-type: none"> • RDS 应由真正意义上的国际第三方提供商运营。 • ICANN 应与 RDS 第三方提供商签订合同以确保数据合规、通过审核和可用。 • ICANN 应与标准验证服务提供商、代理/隐私服务提供商、安全凭证提供商以及其他可能与 RDS 有联系的各方签订适当合同。 • ICANN 应修订现有协议（RAA、注册管理机构协议）以符合 RDS 要求和消除原来的要求。
4.12	存储和托管要求	
	4.12.1 4.12.2 4.12.3	<ul style="list-style-type: none"> • 为了维护冗余系统和消除单点故障，数据应位于多个位置（如注册服务商、注册管理机构、托管和 RDS）。 • 应对托管数据进行审核以检查其格式是否正确，是否完整无遗。 • RDS 应保障数据元的安全性、保密性和完整性，防止有人未经授权而加以利用。
4.13	运营和访问 RDS 的成本	
	4.13.1	<ul style="list-style-type: none"> • 成本问题是 RDS 的一个重要方面。EWG 会对这一问题进行更深入的探讨，包括开发和运营的成本以及支付这些费用的可能方式（如由 RDS 资金支付、用增值服务费抵消）。

V. 建议的模式

出于各种目的收集、存储和披露准确数据元的需求使得 EWG 提出满足第 4 节识别原则的下一代 RDS 初步模式。过去，大多数责任都转移给了以向客户提供有效域名和维系付费客户为首要目标的注册服务商。EWG 认识到，随着互联网生态系统变得愈加复杂，以及数百个新 gTLD 的涌现，新的参与者可能需要承担一些责任，以满足如此广泛的注册数据目的。

根据第 IV 节规定的功能和设计原则，下图 4 说明了 EWG 建议的下一代 RDS 模式，其中可能包含很多这些原则。

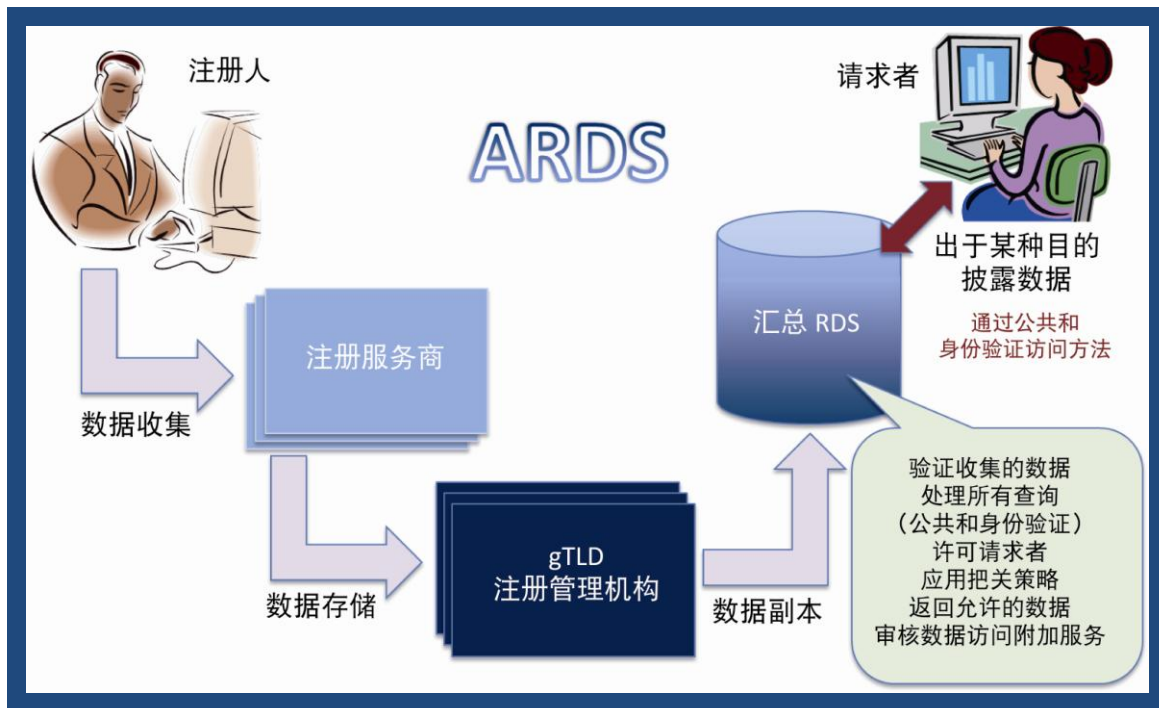


图 4: 集中式 RDS 模式

5.1 多种系统设计的审查

确定为新 RDS 建议的原则和所需功能后，EWG 考量了多种替代模式，以期确定每种模式对已识别的注册数据需求的解决程度。EWG 评估了分布式系统（例如如今的 WHOIS 系统所用系统）和集中式系统。EWG 还考量了一种代理型系统，第三方充当中间方允许对所查询数据的访问，而不充当其存储库。区域文件访问 (ZFA) 咨询小组⁴在新 gTLD 计划背景下考量相似问题，他们的工作对于 EWG 增长这方面的见识极有价值。

分布式系统呈现出的劣势更能由替代模式补足。鉴于成千个注册管理机构可能蜂涌上线，EWG 认识到继续当前的分布式系统会出现效率低下和成本增加的情况，因为请求这些信息的用户可能必须应对各种不同的格式、证书、访问点、许可条款，以及注册管理机构或注册服务商可能设置的其他障碍。正如 ZFA 咨询小组所述：“使用的访问系统不同，区域文件用户实施的流程或自动技术就更容易坏掉。由于用户必须使用唯一的报告系统来解决问题，因此在因故障而导致无法访问时，问题的解决对数据用户来说非常复杂。”⁵ 这些问题应同样适用于 RDS。

此外，支持大力改变数据访问方法并无明显的经济或运营激励，因而与要求每个注册管理机构 and/或注册服务商修改其系统成为实施下一代 RDS 的新分布式系统相关的成本可能限制创新和应用。正如 ZFA 咨询小组所述：

“总体而言，提供对区域文件数据的可靠访问会强制增加 gTLD 注册管理机构的操作成本和责任，而没有直接补偿。注册管理执行机构已将其视为与互联网主要名称空间相关的运营成本之一，因此如果有更有效的方法来提供该访问，注册管理机构必然会采纳，从而降低这些成本。例如，注册管理机

⁴请参考区域文件访问咨询小组的档案以便了解更多信息，网址：

<http://archive.icann.org/en/topics/new-gtlds/zone-file-access-en.htm>

⁵请参考区域文件概念文件，发布地址：<http://archive.icann.org/en/topics/new-gtlds/zfa-concept-paper-18feb10-en.pdf>

构必须向所有购买者提供持续的访问权限，而未指定任何具体的服务级别协议 (SLA)。这显然要花费一些运营资金…注册管理机构还负责向数据消费者提供安全的连接和清晰的数据文件，这就要求注册管理机构创建重要的保护措施。”⁶

另外，分布式或代理型系统难以或不能提供常用功能，例如跨 TLD 注册人查询、反向注册人域名查询，甚至也不能实现历史所有权型注册表。所有这些功能都可能通过收集和维护适用数据的集中式数据库实现。

5.2 建议的集中式 RDS

集中式 RDS (ARDS) 模式（如上图所示）获得 EWG 的共识，认为这是解决上文第 4 节所识别功能需求和设计原则的一种方式。

在提议的模式中：

- ARDS 充当集中式存储库，其中包含收集的所有数据元的非权威副本
- 每个 gTLD 注册管理机构仍然是数据的权威来源
- 请求者申请 ARDS 的访问凭证
- 解除注册服务商/注册管理机构提供端口 43 访问或其他公共访问要求的义务
- 在大多数情况下，ARDS 提供对缓存注册数据的访问，该数据从 gTLD 注册管理机构复制而来，并进行频繁的定期更新
- ARDS 也可以提供对实时注册数据的访问，该数据根据请求从 gTLD 注册管理机构实时获取。ARDS（或与 ARDS 交互的其他第三方）负责执行验证服务
- ARDS 负责审核访问，以最大程度减少滥用，并对不当访问给予处罚或采取其他补救措施
- ARDS 处理数据准确性投诉

⁶请参考区域文件访问概念文件了解更多考虑事项。

- ARDS 管理数据访问的许可协定
- ICANN 与国际第三方签订合同，制定和运营 ARDS，并监控是否符合要求

集中式 RDS 模式	
优点	<ul style="list-style-type: none"> • 通过单一联系点来处理调整工作 • 在传输和递送方面可获得改进 • 为注册数据请求者提供“一站式”服务 • 加强了注册数据验证和访问的问责制（防止滥用） • 能够以相同的方式在多个 TLD 之间跟踪/审核/惩罚请求者（防止滥用） • 可减少注册服务商和注册管理机构当前因提供数据访问而承担的部分成本 • 可提供数据标准化或过滤功能 • 减小了注册服务商和注册管理机构的带宽要求 • 有助于使方法标准化，以解决本地数据隐私权问题 • 提高了跨多个 TLD 的搜索能力（例如反向查询） • 最大程度地减少了过渡和实施成本 • 能够验证/认可具有特殊目的（如执法）的请求者 • 有助于更有效地管理不准确的报告 • 能够进行更有效的随机准确性检查 • 能够以多种语言、脚本和字符显示用户友好的搜索门户网站
缺点	<ul style="list-style-type: none"> • 数据延迟 • 创建了包含极高价值数据的“大数据”源，如果审核和维护不当，可能造成滥用 • 增加了内部人员滥用和外部攻击的风险，需要更加重视安全策略的实施、执行和审核 • 注册管理机构/注册服务商不再控制注册数据的交付

VI. 解决隐私权问题

EWG 权限的重心在于注册数据准确性的问题。如果下一代 RDS 要求大幅提高注册数据的准确性，大量问题就会立刻涌现，其中最具争议的可能是隐私权问题。

EWG 意识到了准确性需求，也认识到了保护可能要求加强个人信息保护的注册人的隐私的需求。能够符合加强保护要求的注册人示例包括受威胁的个人或组织、希望在被广泛认为受保护的互联网上行使自由言论权的注册人，或发言人的身份会威胁自身或家人生命安全的情况。

根据第 4.4 节列举的原则建议，EWG 已讨论了 RDS 可用于满足风险用户需求的方法，亦即使用“安全保护凭证”来最大程度保护注册服务。其中一个方案是，可以使用一套议定标准，让 ICANN 委任一个独立的组织来充当“受信任的代理机构”，由该机构确定注册人是否有资格获得最大保护。EWG 期望深入思考安全保护凭证的潜在模式，这可能有助于在问责制和风险互联网用户的个人数据隐私需求之间找到极具创新性的有效平衡。

VII. 网关访问功能说明

提议的网关访问模式（如图 5 所示）可总结如下：

- 通过 RDS 的一个 web 接口⁷，将细选后的数据元子集公开供匿名请求者访问。
- 所有其他数据元只面向通过 RDS 支持的多模式网关访问方法访问的经验证请求者。
- 网关访问将只提供给申请并获颁 RDS 查询验证所用证书的请求者。本文并未明确颁发凭证所用流程，但是 EWG 建议该流程考虑每个请求者想要访问注册数据的目的。
- 每个网关访问查询将识别经验证请求者的目的（明示或暗示）和所需数据元的列表。只会返回相应域名提供且请求者出于宣称目的可以访问的数据元。

EWG 希望进一步讨论多模式访问方法，以及如何通过现有或未来的注册数据访问协议来启用这些方法。

⁷ EWG 希望进一步探索将一些注册数据元与可以通过浏览器集成访问的网站的域名相关联的可能性。

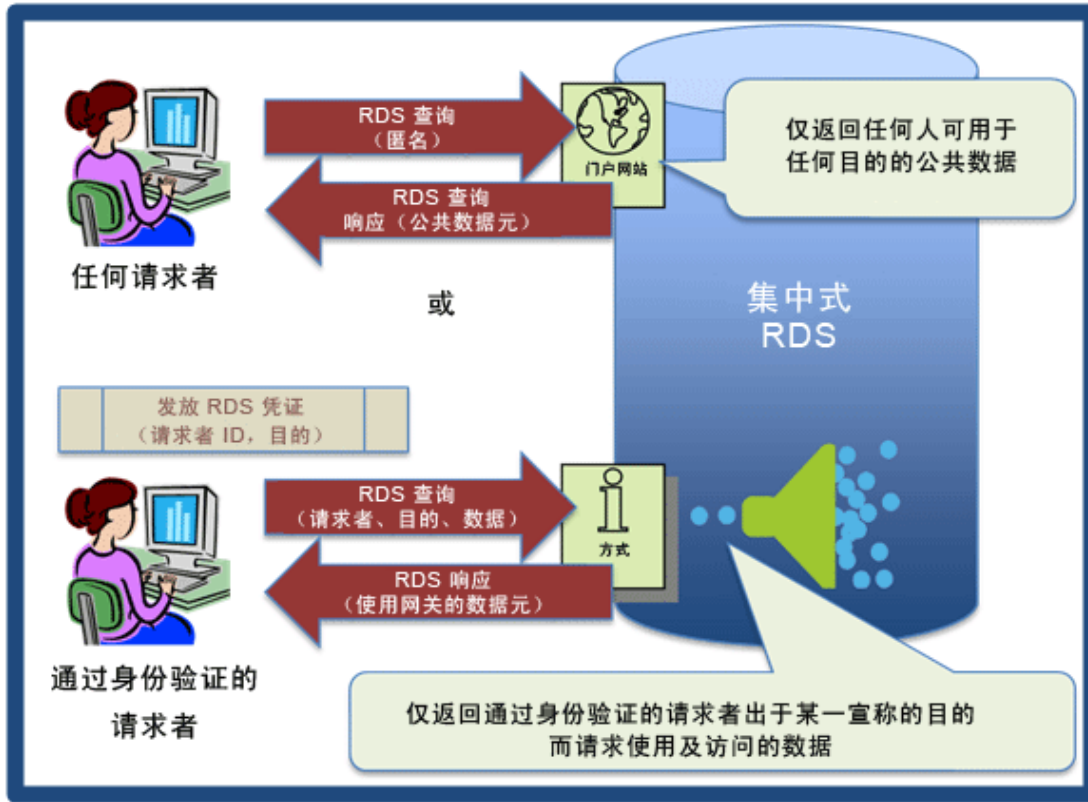


图 5：网关访问模式

VIII. 结语和后续措施

EWG 建议采纳集中式 RDS 而废除当前的 WHOIS 系统，满足 EWG 确定且经本报告更充分描述的设计原则和功能。这包括支持“安全保护凭证”功能，为视为处于风险中的注册人提供加强隐私权保护，例如行使自由言论权的注册人。其中还建议验证收集的注册数据提高准确性，以及通过“网关访问”控制进一步促进问责制（允许具有更多信息需求的请求者申请基于言明目的而有限访问的凭证）。提议的模式并入了旨在处罚请求者试图超出授权级别访问的滥用问题的问责制和审计功能。

重点注意提议的模式体现了源自 EWG 多元化成员资格的艰难妥协，必将不能满足受 RDS 影响的所有利益主体。然而 EWG 希望这些建议整体对当前 WHOIS 系统的巨大推动作用获得公认。

EWG 欢迎大家在线提出公众意见，或就论坛中确定的具体问题在 ICANN 德班会议上与 ICANN 机构群体展开激辩，也欢迎对本报告提出任何更多意见，从而为工作组未来的审议出言献策。在本报告的公众征询结束后，EWG 将再次聚首，深度思考收到的意见，并适当修改其建议。在 EWG 审议结束后，EWG 将发布最终报告并将其提交给 ICANN 首席执行官和理事会，以在适当时作为新 gTLD 政策和合同谈判的基础。如理事会所述，基于最终报告的问题报告将构成理事会发起的、受到密切关注的 GNSO 政策制定流程 (PDP) 的基础。