

SSAD ODP 项目最新进展

SSAD ODP 项目团队

2021 年 11 月 18 日



- 政府咨询委员会 (GAC) 调查结果
- 业务流程设计
- 后续工作
- 问答环节

GAC 调查结果

- 共有 13 份独特的响应：
 - 3 个国家/地区只提供了国家/地区名称
 - 3 个国家/地区完成了部分调查
 - 7 个国家/地区完成了全部的调查

业务流程设计

SSAD 业务流程设计

根据 gTLD 注册数据临时规范第 2 阶段快速政策制定流程 (EPDP) 最终报告中的政策建议，标准化访问/披露系统 (SSAD) 涉及：

8	种参与方类型
8	个子系统
60	项业务流程

SSAD 的参与方

- 数据披露请求者
 - 非政府组织的自然人和法人
 - 政府实体和国际政府间组织
- 认证机构
 - 中央认证机构
 - 国家/地区政府组织认证机构
- 中央网关
- 滥用问题调查机构
- 签约方
 - gTLD 注册管理运行机构
 - ICANN 认证注册服务机构
- 审计机构
- 数据主体
- ICANN 组织

认证机构

- 作为与 SSAD 请求者对接的唯一接口
 - 验证请求者身份
 - 管理披露请求
 - 代表中央网关和签约方对请求者进行验证
 - 管理请求者的账单流程
 - 将请求处理费用转移到中央网关
- 可以将某些职能授权给“身份供应商”
- 政府组织认证机构还必须：
 - 由国家/地区政府指定
 - 实施与中央认证机构相同的接口，以便与中央网关和签约方集成

ICANN 组织提出了四类供应商合同：

1. 系统开发、运营和中央认证机构
2. 中央网关的系统开发和运营
3. 滥用问题调查机构
4. 负责审查请求者活动和认证机构的审计机构

SSAD 子系统



中央网关

1. 网络门户
2. API



认证机构

3. 网络门户
4. API



ICANN 组织

5. icann.org 门户
6. NSp



签约方

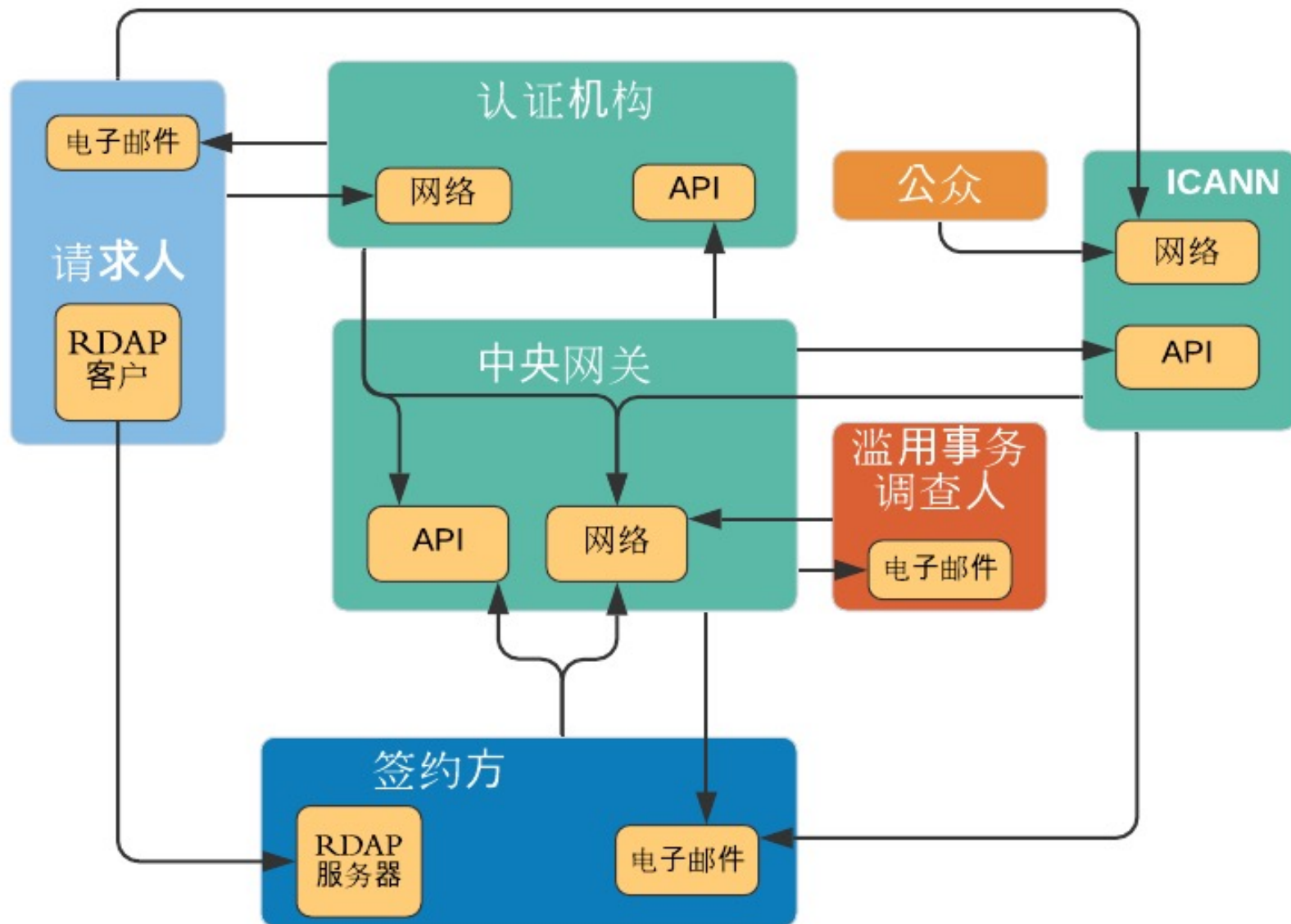
7. RDAP 服务



请求者

8. RDAP 客户端

参与方和子系统交互



- 中央认证机构针对以下内容仅支持英语：
 - 用户界面
 - 披露请求和支持文件
- 政府组织认证机构可以针对以下内容支持任意语言：
 - 用户界面
 - 披露请求和支持文件（如果相关签约方支持）

请求者认证和声明

请求者认证

- 请求者由认证机构认证

 - 必须经过认证才能在 SSAD 中提交数据披露请求

 - 验证请求者身份

 - 认证需要定期更新

- 请求者可以管理验证详细信息，包括：

 - 支持的电子身份证 (eID)

 - SSAD 特定身份凭证

请求者声明

- 经认证的请求者可提交相关声明，供认证机构核实。
- 到 SSAD 启动时：
 - 对于按建议 9.4.1 和 9.4.2 所述自动处理的请求，政府组织认证机构必须支持验证此类请求的声明
 - 中央认证机构将支持验证请求者的商标所有权声明
- 将来：
 - ICANN 组织可能要求认证机构支持其他类型的请求者声明

- SSAD 运营的成本回收方法，体现在以下三种类型的费用中：
 - 认证/身份验证
 - 请求者声明验证
 - 披露请求处理
- 预计由认证机构收取费用
 - 必须将披露请求处理费用转移到中央网关

非公开注册数据披露

- 针对经认证的请求者拟定的数据披露流程分为以下三个异步步骤：

1

经认证的请求者
提交数据披露请求

2

签约方审查请求
并传达决定

3

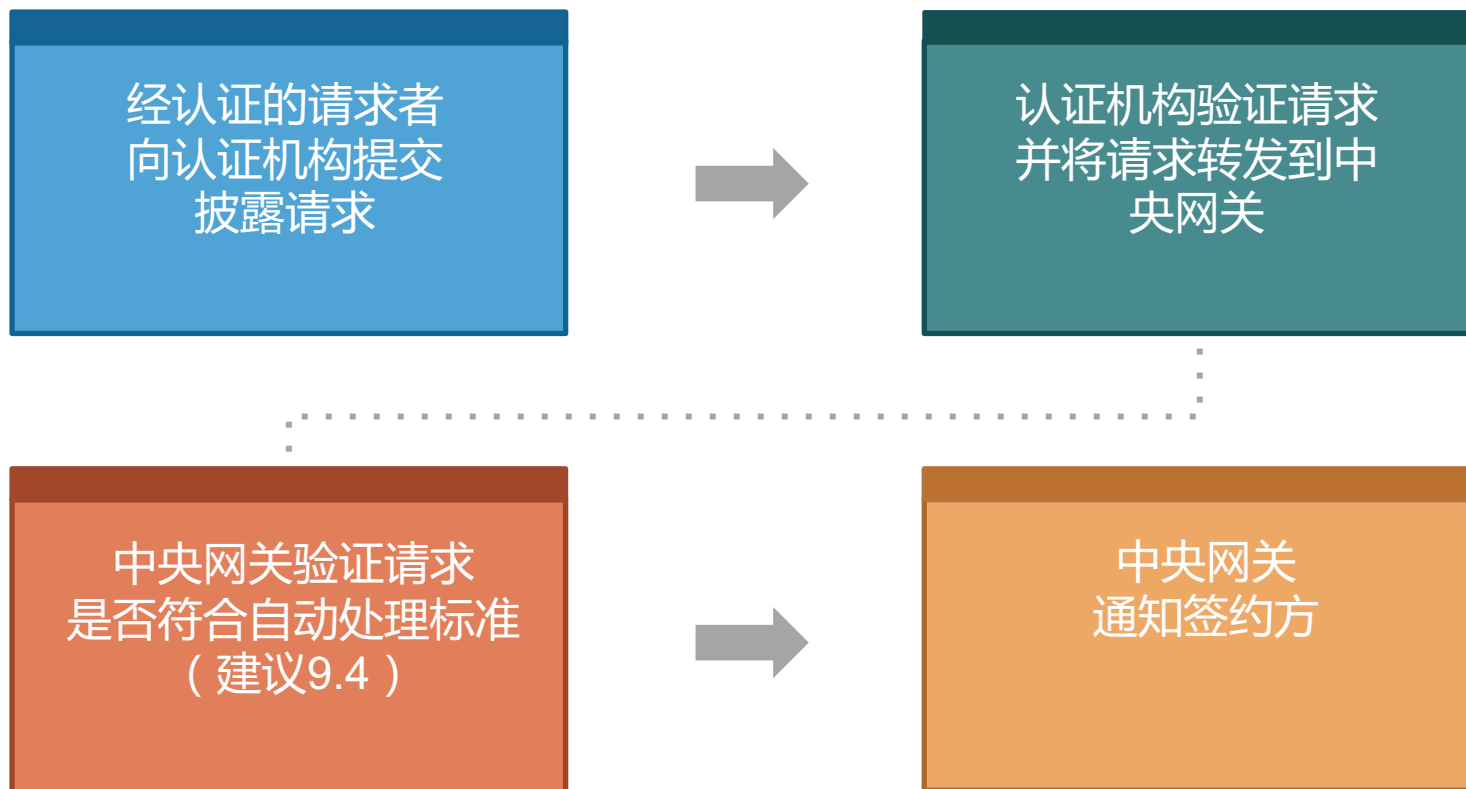
对于已批准的请求，
请求者从签约方的
RDAP 服务中获取数据

非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据



非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

非公开数据披露请求

- 特定域名
- 请求的非公开字段 ([RFC 8982](#) - RDAP 部分响应)
- 请求目的和法律依据
- 请求优先级
 - 紧急
 - ICANN 行政诉讼程序
 - 其他请求
- 支持文件
- 经验证的请求者身份 (姓名、组织、国家/地区)
- 经验证的请求者声明 (如适用)
(以签名的 JSON Web 标记的形式传输)
- 保密等级

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

披露建议引擎

- 中央网关可以选择为签约方实施建议引擎，以决定是批准还是拒绝披露请求。

为了实施 ODA，该设计在 SSAD 启动时不考虑建议引擎。

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

披露请求处理的自动化

- 最初，自动化的范围仅限于建议 9.4 中列出的 4 个情景
- 中央网关将不支持在不进行额外系统开发的情况下为自动化处理添加情景

未来纳入其他情景（例如其他数据保护法）需接受 GNSO 常任委员会的审查

签约方可以根据自己的政策和适用法律自动处理披露请求

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

自动化处理的豁免

- 签约方可以请求豁免自动处理建议 9.4 中任何特定类别的披露请求
例如，当法律不允许时，或者发现重大风险时
必须提供支持文件以供 ICANN 组织审查
ICANN 组织可以撤销豁免（根据建议 9.5）
- 签约方可以根据以下具体情况选择退出自动处理：
域名
请求者管辖权

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

自动审批披露请求

- 满足自动处理标准的披露请求将被视为在中央网关中自动获得批准，除非签约方：
 - 之前已通知 ICANN 组织其需要豁免自动处理
 - 之前已选择退出相关域名的自动处理
 - 之前已选择退出对来自相应司法管辖区的请求者的自动处理
 - 请求者因自动化而受到制裁，或正在接受 SSAD 中潜在滥用行为的调查
- 所有其他请求将转发给签约方进行人工审核。

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

披露请求传递

- 中央网关通过 API 以电子邮件和轮询消息的形式通知签约方
- 默认情况下，会将请求发送到域名的赞助注册服务机构，但详尽注册的情况除外：

请求者要求发送给注册管理运行机构

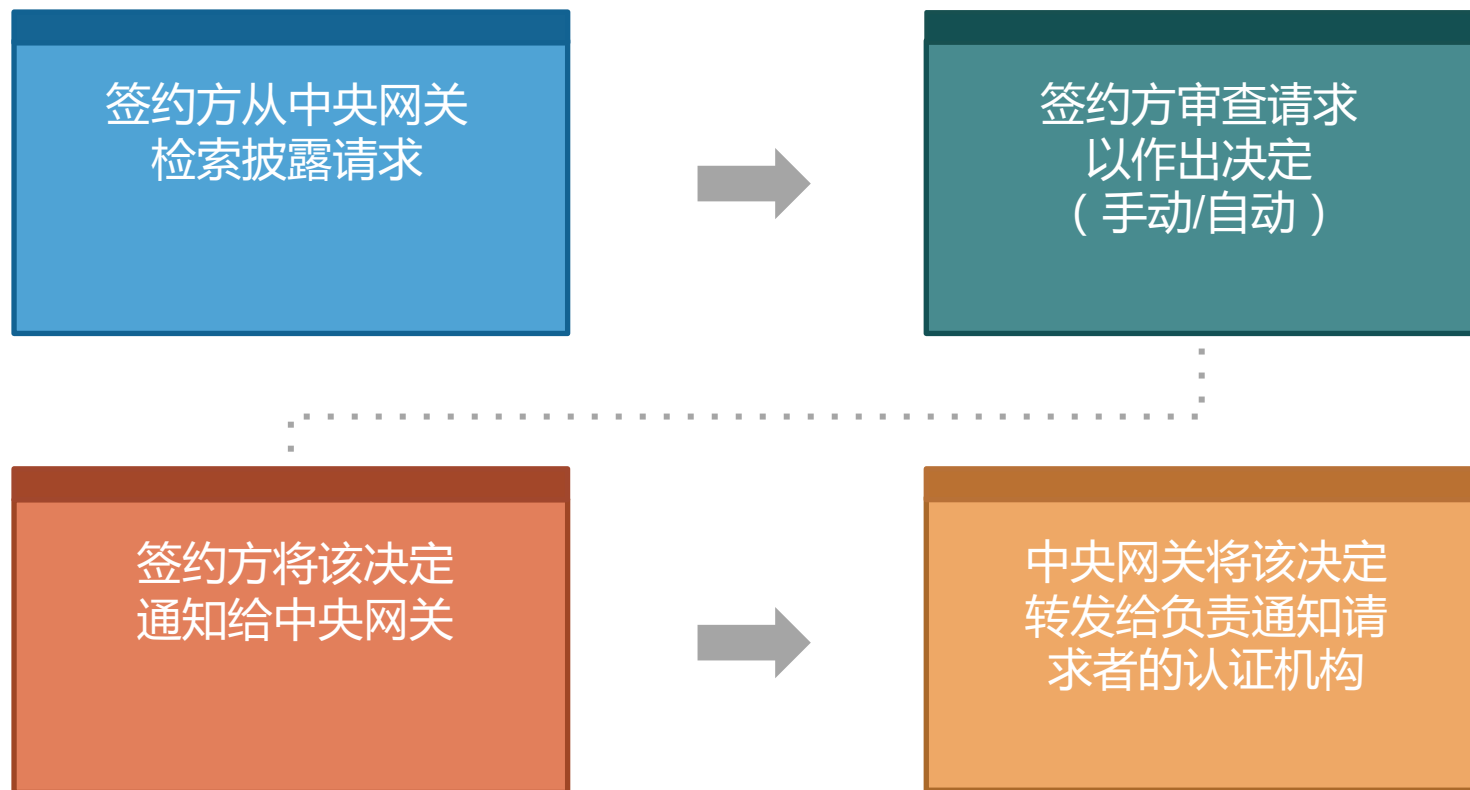
注册服务机构 RDAP 服务不可用

非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据



非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

签约方与中央网关的集成

签约方可通过以下方式与中央网关集成：

- 网络门户

预计交易量较低

- **API**

适用于喜欢系统集成的签约方

请求处理量较大

非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

披露请求检索

- 签约方从中央网关检索披露请求，包括：
 - 请求详细信息
 - 表明是否满足自动处理标准的指示信息
 - 中央网关提供的批准或拒绝建议（如果已实施）

非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

披露请求决定

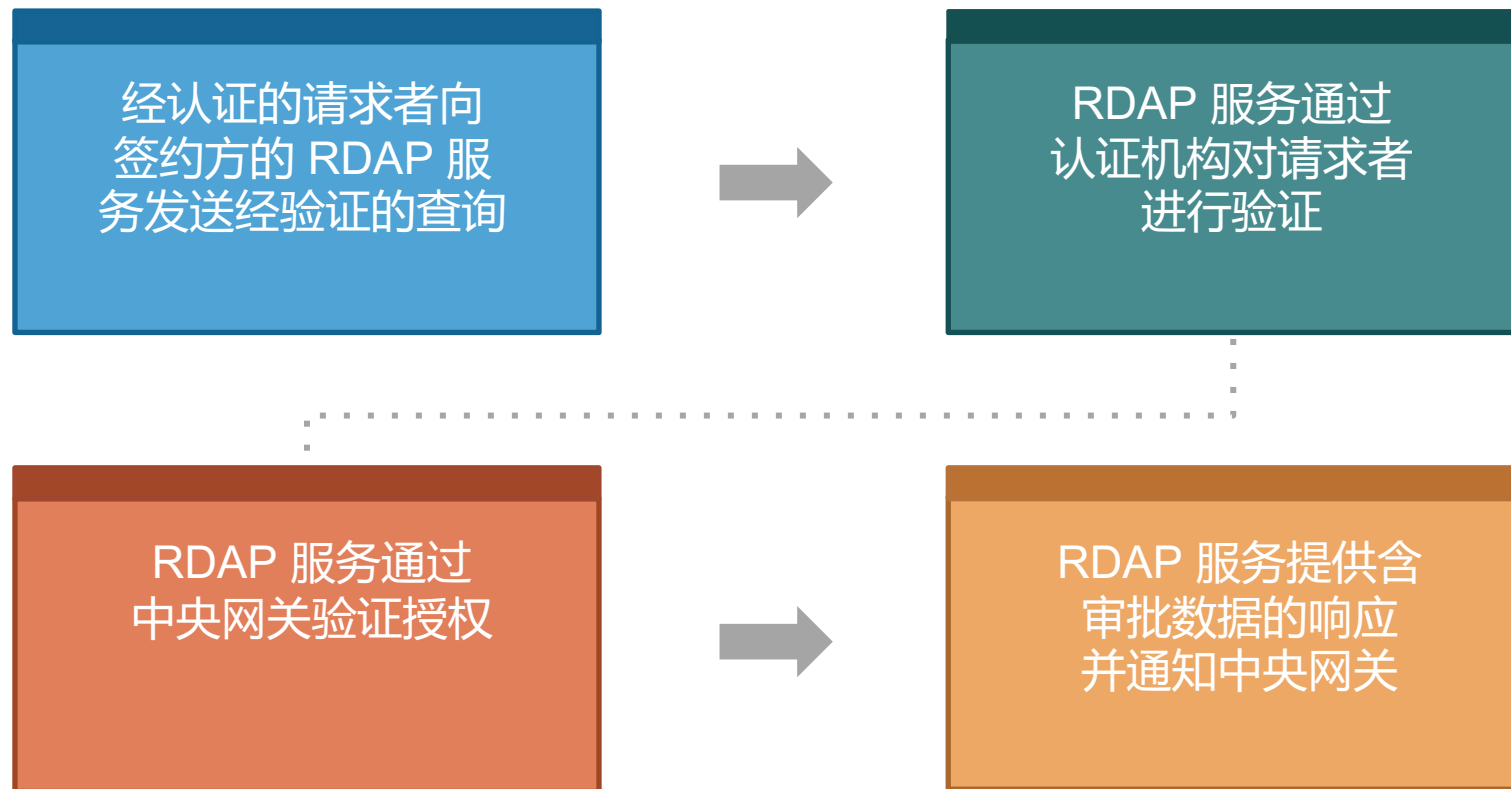
- 签约方是其数据披露请求的唯一授权人
- 一旦请求被审查，签约方必须向中央网关报告：
请求决定（批准、拒绝或其他必要信息）
披露请求是否被批准，因为域名注册数据不包含任何个人资料

非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据



非公开注册数据披露

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

请求者验证和授权

- 认证机构必须支持使用 [OpenID Connect](#) 对请求者进行联合验证
- 基于 [TSG01：访问非公开注册数据的技术模型](#) 的建议设计：
 - RDAP** 服务运营商接收非公开数据请求验证的请求
 - 认证机构提供用户验证服务
 - 中央网关确认授权是由签约方提供的
 - 如果验证和授权成功，**请求者**将收到含非公开审批数据的 RDAP 响应

1. 提交数据披露请求

2. 审查数据披露请求

3. 披露已批准请求的数据

增加了对 RDAP 服务的要求

- 在与签约方进一步讨论后，RDAP 服务运营商必须支持：

基本 RDAP 标准

[Draft-ietf-regext-rdap-openid](#) - 使用 OIDC 的 RDAP 联合验证

[RFC 8982](#) - RDAP 部分响应

- 必须定义字段子集

更新了 gTLD RDAP 简介

请求者和签约方的合规实践

SSAD 中的合规实践

- SSAD 滥用问题调查机构负责：
 - 监控标准运营衡量标准
 - 监控请求者对 SSAD 服务条款的遵守情况
 - 验证滥用报告
 - 来自签约方
 - 来自数据主体/公众
 - 提供请求者的补救机制 (建议 13.1.3)

- 合同合规部负责调查：
 - 签约方在 SSAD 中的潜在滥用行为
 - 上报不遵守 SLA 的情况

- 由于 SSAD 中的滥用行为，滥用问题调查机构可能会确定分级处罚：
 - 限制处理所允许披露请求的速率
 - 排除在披露请求自动处理范围之外
 - 暂停请求者认证
 - 撤销请求者认证
- 请求者可以对处罚提出上诉
 - 由滥用问题调查机构进行审查

- 由独立审计机构执行
- 审计周期：
 - 运营前的初步审核
 - 随后根据以往的审计结果进行年度审计
- 审计范围：
 - 请求者
 - 基于提供给中央认证机构和中央网关的文件
 - 中央认证机构
 - 指定的国家/地区政府组织认证机构
 - 可以选择使用他们自己的审计机构

其他系统要求

服务水平协议 (SLA)

- 中央网关和中央认证机构系统预计遵循以下 SLA :

SLA	说明
99.9%	系统可用性
≤ 4 秒	系统响应时间, 95% 的查询
24x7	英语客户支持

系统日志记录和数据保留

- 预计由 SSAD 中的子服务提供商制定记录程序：
 - 中央/政府组织认证机构
 - 中央网关
 - 签约方
- 预期的数据保留策略是将所有运营数据和系统日志总共保留 **18 个月**

- **每季度**通过 ICANN 组织门户发布，至少包括以下内容的摘要
详细信息：

收到的披露请求数量

- 批准/拒绝
- 自动/手动
- 第三方目的/理由
- 优先级和平均响应时间

关于 SSAD 财务可持续性的信息

最新 EDPB 指南或最新法学理论（如果有）

技术或系统难题

运营和系统加强机制

反馈

为社群提供反馈的机会

- 我们是否采取认证建议中列出的所有必要措施、提交披露请求并将其发送给签约方？
- 此模型中是否缺少任何参与方或子系统，或者您认为应该包括但尚未确定的角色与责任？



请提供您的反馈！

- 通过 odp-ssad@icann.org 接收和分析社群反馈
- 下一次网络研讨会计划于 2021 年 12 月举行

有问题？



与 ICANN 展开交流



谢谢

<https://www.icann.org/ssadodp>

电子邮件：ODP-SSAD@icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg