
ICANN
COMMUNITY FORUM
64
KOBE
9–14 March 2019

# Technical Study Group on Access to Non-Public Registration Data

**Ram Mohan, Coordinator**

ICANN64 (Kobe)
11 March 2019

# Agenda

- Background
- Use Cases
- System Requirements
- Proposed Model
  - Draft Design Schematic
- Assumptions
- Timeline
- Considerations
- Questions

# What Is The Technical Study Group (TSG-RD)?

Home Page: https://www.icann.org/tsg

**TSG Charter**: Includes Purpose, Assumptions, Key Questions and Considerations

**Motivation and Background**:

1. Balance data protection requirements with legitimate interests of third parties to access non-public gTLD registration data
2. Intent to reduce potential liability faced by gTLD registries and registrars when providing such access

**TSG Purpose**:

Explore technical solutions for authenticating, authorizing, and providing access to non-public registration data for third parties with legitimate interests, built on the Registration Data Access Protocol (RDAP)

**TSG Remit**:

No decisions or recommendations on policy questions (e.g., who gets access, which data fields, under what conditions should access be given, what is a legitimate interest, etc.)

# Who are the TSG-RD?

| Role | Name | Affiliation/Employer |
|---|---|---|
| **Sponsor** | **Göran Marby** | **ICANN** |
| **Coordinator** | **Ram Mohan** | **Afilias** |
| **Team Members** | **Benedict Addis**<br>**Gavin Brown**<br>**Jorge Cano**<br>**Steve Crocker**<br>**Scott Hollenbeck**<br>**Jody Kolker**<br>**Murray Kucherawy**<br>**Andy Newton**<br>**Tomofumi Okubo** | **Registrar of Last Resort**<br>**CentralNic**<br>**NIC Mexico**<br>**Shinkuro**<br>**Verisign**<br>**GoDaddy**<br>**Facebook**<br>**ARIN**<br>**DigiCert** |
| **ICANN Org Support Team** | **Eleeza Agopian**<br>**Francisco Arias**<br>**John Crain**<br>**Daniel Halloran**<br>**Gustavo Lozano**<br>**Diana Middleton**<br>**Erika Randall**<br>**Yvette Guigneaux** | **ICANN** |

# TSG Process

ENGAGEMENT MODEL
Consensus driven, iterative, technical focus

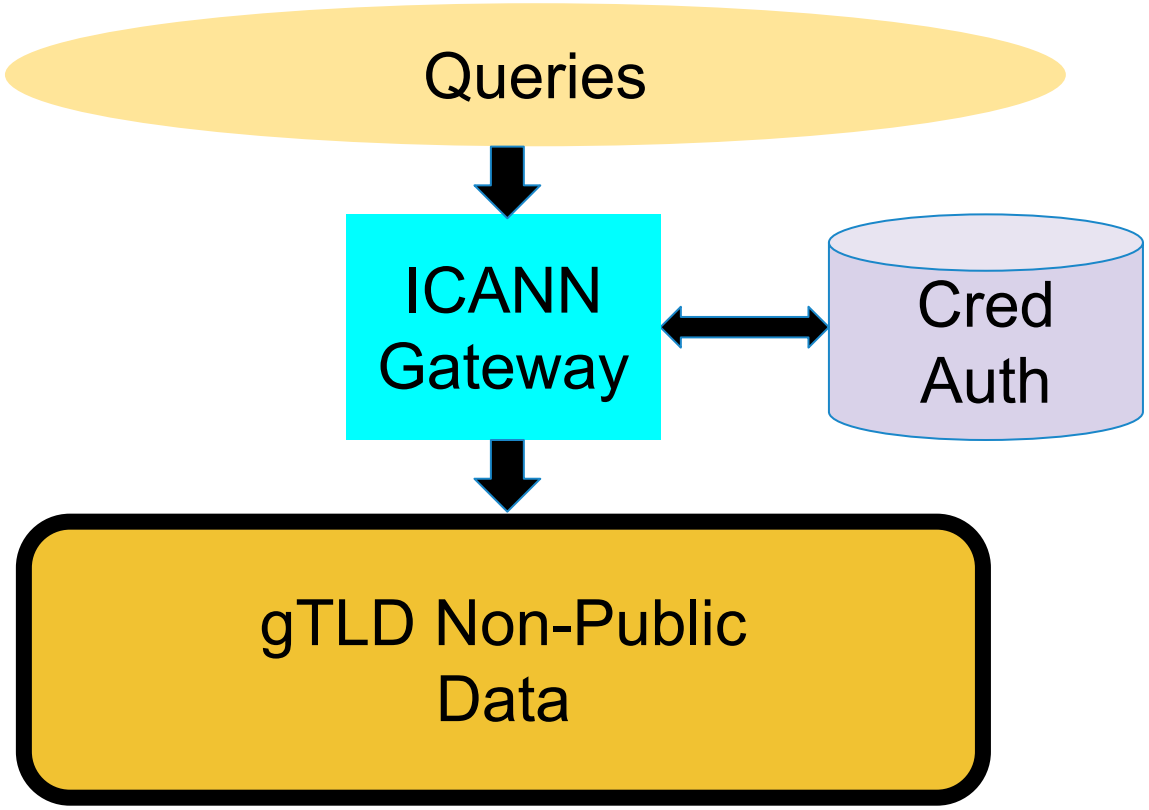
1. Define **key questions** and considerations
2. Identify main **assumptions**
3. Identify **use cases** & user journey
4. Define system **requirements** (functional, operational, management)
5. Create functional requirements and mapping
6. Build actor models
7. Determine implementation considerations
8. Arrive at proposed **solution** (the Technical Model)
9. Notify **considerations** for other entities and organizations
10. Invite community feedback
11. Review and revise Technical Model

# Key Questions & Considerations

Major categories:

- Assessment of Available Tools & Protocols
- Authentication/Authorization
- Data Transport/Storage & Audit
- Access Control Protocol
- Performance Requirements
- Transparency, assignment of responsibility:
- Error conditions
- Accounting, costs, billing
- Maintenance and evolution
- Governance and oversight of system
- Multi-use requests

# Assumptions




ICANN reduces gTLD registrars' and registries' GDPR liability

(1, 2) RDAP is the mechanism; port 43 deprecated
(3) Access to gTLD Non-public data only via ICANN
(7) Queries from unauthenticated sources per policy
(5, 10) ICANN oversees credential protection and validity

# Twelve Assumptions

(1) RDAP will be used; adios port 43
(2) Everyone will use
(3) ICANN is only path
(5) Credentials protected
(7) Unauthenticated queries via policy
(10) ICANN ensures validity of credentials

System must evolve/fit to…

(4) Changes in data sets, rules
(6) Match normal RDAP usage
(8) Existing RDAP practices
(9) Pilot experience
(11) Policy choices
(12) Implementation practicalities

# Five Use Cases

- Use Case #1: Authorized users (e.g., security researchers, law enforcement, registrars, registries, etc.) require access to domain records, which might include single queries or multiple queries. (Critical/Must have)
- Use Case #2: User receives authorization online and gets data immediately. Authorization can be broad and ongoing, or specific and constrained. (Critical/Must have)
- Use Case #3: Unauthorized, unauthenticated users request access to data elements associated with domain records. (Critical/Must have)
- Use Case #4: Authenticated user requests data for which user is not authorized. (Critical/Must have)
- Use Case #5: Data subject requests their own data via this system. (Useful/but not necessary)

# System Requirements

1. Overall: Based on current Internet standards; support IPv4 & IPv6; support a distributed data model; use TLS and other appropriate secure protocols

2. ICANN Browser-based Web Portal: System accommodates “exceptional” requests for human review; provides support for high-priority requests; assign requestor ID; associate requetor attributes

3. Authentication and Authorization Determination: May be delegated to qualified agents appointed by ICANN org

4. ICANN RDAP Gateway: Must support multiple authenticated requestor identities and multiple authorization policies; must allow granular access to various data elements; must support passing requestor attributes and identifiers to contracted parties; redirect unauthorized queries; allow automation

5. Contracted Party RDAP servers: Must receive and respond to queries from ICANN with all available registration data

# System Requirements (cont.)

6. Logging/Auditing: All parties must securely log query data, which must be attributable to a user; data retention must be supported; there must be a means to reconcile queries between the parties

7. Performance/SLA: Must be SLA commitments for all the service subsystems' availability, and Web-based interface request resolution times

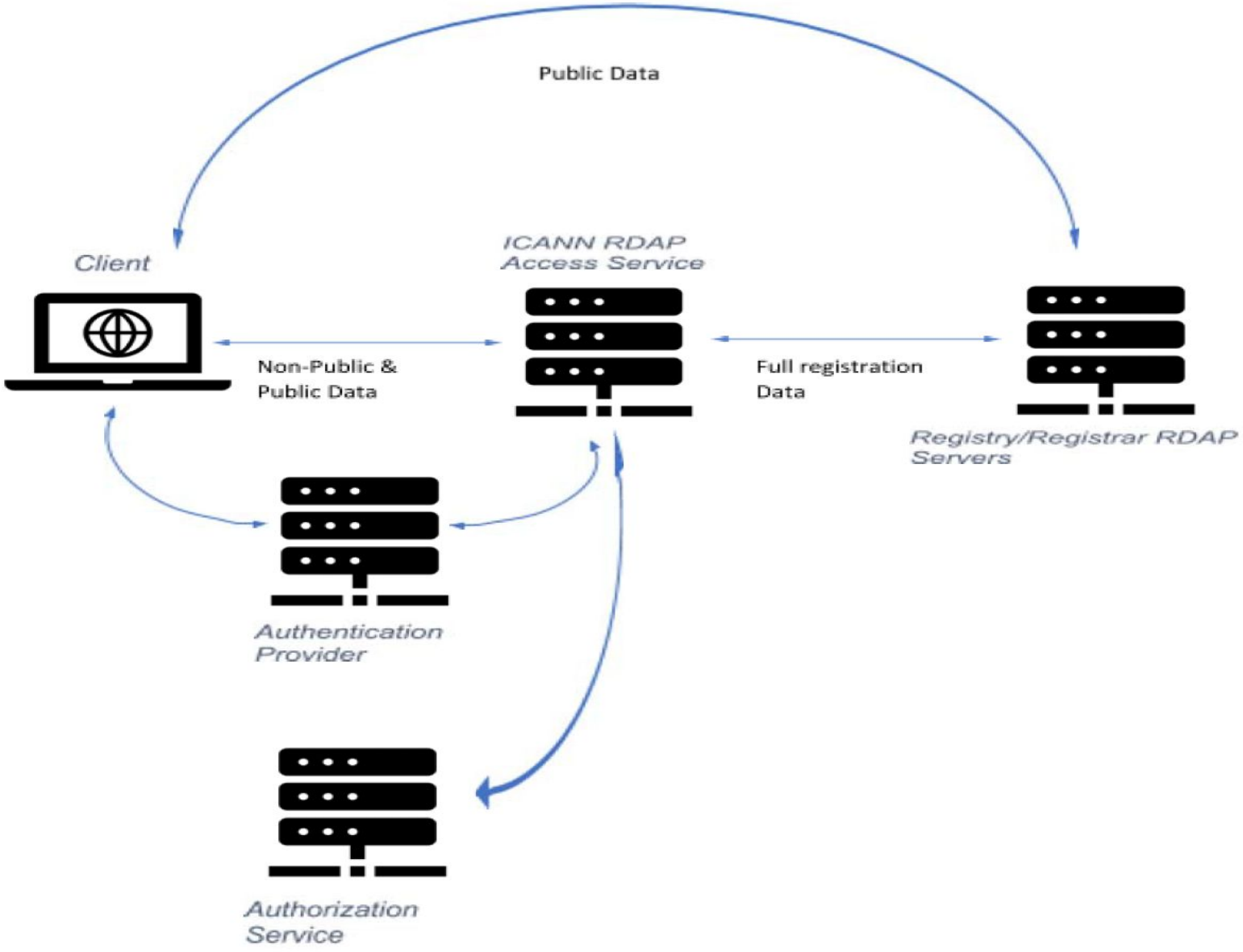
8. Information security requirements: Security controls should be based on risk assessment; ICANN org and Identity Provider must undergo an annual security audit and provide an audit report on request; must be a mechanism for reporting breaches; all parties to abide by best current practices

9. Information security guidelines: Must be governed by a business continuity management program; cryptographic techniques should be adopted to protect confidentiality and integrity of the data

# Proposed Model: RDAP with OAuth 2.0 and OpenID Connect

- Prerequisites
  - Service providers exist and can exchange configuration information
  - Requestors are issued credentials by an Identity Provider
- Access Request
  - Requestor uses client to send RDAP request to Access Service
  - Access Service redirects client to Identity Provider
- Identification and Authentication
  - Identity Provider prompts for credentials, identity attributes, and consent
  - Requestor responds, <submit>
  - Identity Provider returns code and redirects client to Access Service
- Setup for RDAP Query
  - Access Service uses code to retrieve tokens from Identity Provider
  - Tokens are returned to the client
  - Client sends RDAP query and tokens to ICANN RDAP Gateway
- RDAP Query Processing
  - ICANN RDAP Gateway receives query and tokens
  - Gateway sends query and tokens to Authorizer for verification
  - Authorizer processes inputs and returns verification result
  - (If authorized) Gateway sends RDAP queries to Contracted Party RDAP servers
  - Gateway processes and filters responses
  - Gateway returns RDAP response to client
  - Client displays result to Requestor

# Draft Design Schematic



# Considerations

1. Data Retention: Any data stored by these systems should be regulated by policies developed outside of the TSG and communicated to the data processors, audited and enforced.

2. SLAs: Contracted parties will be subject to SLAs for their own RDAP services. However, ICANN org as the operator of the RDAP Gateway, Identity Providers and Third Party Authorizers should also be subject to SLAs. It is also RECOMMENDED that ICANN org provide transparent reporting on the service level performance of each of the actors in the system.

3. ICANN Org Obligations: ICANN org should review the operational outcomes of operating such a system to determine feasibility as well as operational and financial impact. ICANN should also publish this review for public comment.

4. ICANN as Coordinating Party: ICANN may be exposed to significant operational and legal risks if ICANN will be credentialing requestors. ICANN should identify, assess and take steps to mitigate these risks.

# Considerations

5. Risks to Contracted Parties: The TSG cannot comment on whether the new system reduces or increases the risk to contracted parties. It will be up to the contracted parties to determine their own risk based on their own legal advice.

6. Transparency: It is recommended that ICANN publish a regular report that provides statistics for request for access to non-public gTLD registration data.

7. Mechanism For Handling Complaints: Users should have a means to escalate their requests if they are denied through a complaint process. ICANN org should also have a process for deleting data under Article 17 of the GDPR.

# Timeline and plans

- ICANN64: Community input to be incorporated into the draft Technical Model
- March-April 2019: TSG-RD continues discussions to finalize Technical Model
- 23 April 2019: Final Technical Model published

# Contact the Technical Study Group

Home Page: https://www.icann.org/tsg

email: gdpr@icann.org

# Engage with ICANN

## Thank You and Questions

Visit us at **icann.org/tsg**
email: gdpr@icann.org


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


slideshare/icannpresentations


soundcloud/icann