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

# Face-to-Face Meeting #2, Washington, DC

#### 

#### **Monday, 11 February 2019**

Technical Notes

The group discussed the appropriate response for unauthorized queries in the ICANN RDAP Proxy. Gavin suggested that an error may be an appropriate response. The general feeling of the group is that a redirect to the appropriate party based on the IANA bootstrap is the appropriate response, but there are scenarios where an error may be the appropriate response, therefore 4.g changed to MAY instead of a MUST.

The group discussed how to know (in-band) what elements the user is authorized for before making a query. Scott explained that in core RDAP this is not supported; in RDAP the user needs to make a query and the server creates the response based on server policy.

4.c, Francisco explained that the system must support the use case of a requestor authorized for an specific query. 4.c was changed to support this scenario.

5.a. Francisco explained that dictating requirements to the CPH’s RDAP servers is not part of the scope for this group, and is covered by an agreement between ICANN and CPHs. Scott explained that the model requires some mention about the expectations of the CPH’s RDAP servers. Gavin explained that the charter mentions the expectation regarding the treatment of public data queries on the CPH’s RDAP server. 5.a. Changed to only cover the communication between ICANN and CPH’s RDAP servers.

6.a The group agreed to modify the text to reflect that all parties shall keep the auditing and logging data secure.

6.c Francisco: requiring logging data not being publically is a policy decision. Andy: a requirement of making logging data publicly available will conflict with other requirements. The group agreed change the MUST NOT to SHOULD NOT.

6.d The group agreed that statistics should be aggregates and not identify a particular entities.

6.e. Gavin suggested to convert the text (currently a suggestion) into a requirement. The group discussed if the group can create requirements for policy-developers. The agreement is that we should say what is needed, and the policy-developers may decide to ignore.

The group discussed about publishing performance with SLA requirements. Francisco explained that ICANN has shared aggregates about performance of contracted parties with the SLA.

The group discussed the purpose of the requirements of the information security section, and the sentiment is that the audience of the document expects security commitments to be present in the document.

Benedict suggested to reference Article 32 of GDPR for risk assessment. Gavin suggested to not reference an specific piece of legislation that may not apply everywhere, therefore Article 32 of GDPR is listed as an example.

Benedict suggested that the infosec controls shall also cover the requestor (e.g. agreeing to some code of conduct). The group agreed to add this as a hard requirement to the Assumptions section in the charter document.

The group agreed to split the information security sections into two: guidelines and requirements in order to define hard requirements.

The group agreed to add an assumption regarding the right to be forgotten to the Assumptions section in the charter document.

The group discussed RDAP Model 1 that rely on OpenID connect. Steve ask to identify in a potential swim lane diagram what is human driven and what is automated. Additionalty identify which protocols are used in each interaction. Layout the normal case and the error case.Scott explains that the diagram that he proposes in the RDAP 1 model document is a high-level projection for making easier to understand to non-engineers.

Gavin explains that the proxy can provide a cookie to maintain the session with the RDAP server for subsequent queries.

Steve suggests to separate the process of authentication/authorization and making the query once a token is known.

The group discussed how a non-browser client will work, and agreed to explore how this would work.

Scott explains that the identity providers will produce a custom token based on the type of user group for letting the RDAP server make decisions based on the type of user groups. For example, a law enforcement identify provider.

Francisco explains that there are two models to be supported: when the user agent is pre-authorized for any query, and when the user agent is authorized for one particular query. Steve explains that the second case is just another case of an unauthorized query.

Jody asks the group who is the entity making the authorization decision about a particular query. Francisco explains that multiple entities may provide authorization.

The group discussed the use cases for which TLS client certificates may be used.

#### **Tuesday, 12 February 2019**

Technical Notes

The group discussed a model with TLS-client authentication. The group decided to call the TLS-client authentication, model 1.b. OpenID Connect would be called model 1.a.

3.a. The group agreed that the models should accommodate one-time queries and B2B, therefore model 1.b is deemed to not comply with this requirement.

6.c. The group agreed to modify 6.c to mention that the availability of this feature is dictated by policy.

The group discussed if supporting TLS-client certificates or shared secret (e.g. passwords) should be policy or a decision of the IdP. The group discussed if the user should be making the decision between using certificates or shared secret (e.g. passwords). The group agreed that IdPs should support one and/or both technologies TLS-client certificates / shared secrets. The group agreed that IdPs should make a decision between using TLS-client certificates / shared secrets.

The group discussed how to pass the pseudo-anonymised ID when different models are used: 1) OpenID connect between the end-user and the RDAP proxy, and 2) TLS-mutual authentication between the RDAP proxy and the CPH.

The group discussed if a decision should be made about two potential operational models: 1) ICANN is the only IdP, or 2) the IdP function (with the possibility of authorization being delegated to a different party) is done by a third-party. The group decided to describe all potential permutations models in the document.

*Discussion with Goran*

Goran notes that group should discuss options available within the models, time permitting and those that may be significant options.

How do you have a system where a credential can be revoked? Goran says there should be ramifications for not following the rules of the system.

#### **Wednesday, 13 February 2019**

Technical Notes

The group discussed the complexity on the implementation that each party (i.e. end-users, cph, icann, idp) should absorb.

Scott asked the group why we have been focusing on CLIs if end-users use browsers. Andy explained that the idea was to take the hardest case. Gavin mentioned that the complexity of a system increases the possibility of bugs.

The group analyzed two ways of implement the generation of the access / id token: 1) in-line with the rdap query <-> response flow between the end-user and the icann proxy, 2) up-front before contacting the rdap proxy with the rdap query.

The group preference is for doing autohrization/authentication up-front before doing the RDAP query.

Gregory Mounier and Jean-Charles Schweitzer of Europol joined the discussion. Discussed authentication and authorization for law enforcement. They say web-based authentication would be easier. Discussed Europol as an identity provider for its member states.

Action Items

* Entire Group to make edits to their sections in Working Draft document BEFORE next week’s meetings (19 & 21 February)
* Eleeza to add additional assumptions to Charter from Working draft document - DONE
* Eleeza updates to Working Draft outline - DONE
  + to add text as required from charter and other documents.
  + Eleeza to incorporate diagram 1 from this [page](https://medium.com/@darutk/diagrams-of-all-the-openid-connect-flows-6968e3990660) into draft technical model document
* Eleeza/Diana for Meeting #? Dated 5 March:
  + Schedule agenda item to discuss Conclusion section
* Calendar Invites - DONE
  + Yvette to send 21 Feb 90 minute meeting calendar invite
    - Agenda item: do we need call next week?
  + Yvette to send 26 Feb 90 minute meeting calendar invite
  + Yvette to update 5 Mar meeting invite to 60 minutes (not 120 minutes) - same start time
  + Yvette to send 2 & 4 April 90 minute meeting calendar invites
  + Yvette to update 9 April meeting invite to 60 minutes (not 120 minutes) - same start time
* Eleeza/Diana to send invite to SO/AC/SG/C leaders for meeting with TSG - DONE
  + Limit sessions with community to 45 mins, with a 20-25 min presentation from team and leave remainder of time for discussion.
* Eleeza to update presentation with material we created in this session and add to the team drive - BY 26 FEB
* Diana to create archive folder and move old docs into the archived area - DONE
* Eleeza to touch base with Legal regarding Assumption #12 - BY 21 FEB
* Eleeza to add link to Requirement #8 - DONE
* John/Gustavo to check uniformity of language in doc -- specifically “coordinating party” references - BY LAST MEETING BEFORE KOBE
* Diana to publish Charter with redlines - in conjunction with blog - WEEK OF 18 FEB
* Diana to publish proposed RDAP Model - in conjunction with blog - WEEK OF 18 FEB
* Diana to publish updated Requirements with redlines - in conjunction with blog - WEEK OF 18 FEB
* Yvette to publish meeting recordings - DONE
* Diana to send meeting notes to mailing list - DONE