Use Cases for Technical Study Group on Access to Non-Public Registration Data

Use Cases	Critical (Must have)	Important (Nice to have)	Useful (But not necessary)	Comments
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. This does not preclude a later mechanism supporting bulk queries and replies. Reverse search capabilities are contemplated, but the TSG recognizes that this is an advanced search capability that is not fully supported at this point in time.	x			GB's presentation: http://regiops.net/wp-content/uploads/2018/05/8-ROW7_RegistrantID.pdf
Use Case #2: User receives authorisation online and gets data immediately. Authorization can be broad and ongoing, or specific and constrained.	x			
Use Case #3: Unauthorized, unauthenticated users request access to data elements associated with domain records	x			
Use Case #4: Authenticated user requests data for which user is not authorized.	x			
Use Case #5: Data subject requests their own data via this system.			x	May present technical challenges. Could be handled manually, no plan to design this system for this use case. Expected low volume, expected difficulty in assigning tokens to individuals, etc.

User Journey

User should be able to discover the base URL for the centralized access and authorization system
Correlate based on different aspects without seeking access to the underlying data. (eg., i can't tell who registrant is, but i can tell they are the same. Was name just registered? Registered to someone I've seen before? An abusive registrant?)
Authorization is centralized within ICANN. Access of GDPR-protected data is centralized within ICANN
Users who have no authentication vs. wrongly authenticated. A lightweight mechanism to redirect such users properly

Unicorns

Notes

User attempting to find a relevant party with a bad actor's IP address. Use RDAP to find the server? We note that in this case this is already public data; the data is available through conventional means				

ICANN needs to be ready to build and manage a system that moderates access requests, at scale, with SLAs etc. attached to it? **To be raised explicitly in TSG report, with sufficient visibility for ICANN community, Org and Board**
The design and engineering parameters of the system should be cognizant of the policy changes ICANN adopts.
Logic living centrally (mapping of profiles, etc.) may be a good design goal - simplifies things, helps with discoverability, etc.

Questions to Goran

Is ICANN going to be the single responsible party for all non-public data queries? Taking into account the legal and political implications that involves? Or is a distributed model also a possibility?	Answer: Yes, that's the working theory
Is ICANN the sole party authorizing access to non-public data in the gTLD context?	Answer: Could be delegated? Managing of volumes is what creates the problem
Can CPs have visibility into the requests/the justification for the data requested?	Answer: Transparency question. Yes, so long as it doesn't increase risk to the contracted parties.
Would ICANN be open to publishing a transparency report on non-public data queries?	Answer: Depends on the law. Generally, no problem on principle. Ultimately depends on policy