Accreditation & Access Model
For Non-Public Whois Data
March 12, 2018
Version 1.1

Introduction & Overview

This document provides a framework for the rapid implementation of a certification and access model for non-public Whois data for legitimate and lawful purposes[1].This model specifically excludes law enforcement agencies (LEA) and other governmental access, though such access could be provided and validated in a similar fashion. Elements included in this model:

- the types of eligible entities that may seek access to data;
- legitimate and lawful purposes for accessing data;
- how eligible entities may be accredited to access data;
- a proposed operating model and
- terms of accreditation.

Under this model, defined groups of organisations or categories of organisations can gain access to gated data if they (1) require access to data for specific, legitimate and lawful purposes, and (2) are properly validated by a third-party accreditor.

This descriptive document is intended as the basis for creation of a functional specification for implementation. (For a similar approach, see the TMCH Functional Spec Example[2])

Eligible Entities & Eligibility Requirements

Eligible entities highlighted here for this purpose are derived from the entities and use cases documented in the Expert Working Group's final report on gTLD Directory Services.[3] As such, the three Eligible Entities discussed here do not represent the finite universe of all possible Eligible Entities, but include those having legitimate and lawful purposes to access data, as well as agents that facilitate protection of public interests, security and lawful behavior alongside Eligible Entities.

1. Cybersecurity & OpSec Investigators

Eligible Entities would include individuals and companies who provide cybersecurity or operational security for themselves, a corporation, or provide it as a solution and/or service to other individuals or entities. Examples of such services include:

- security intelligence and analytics;
- identity and access management;
- application security;
- fraud protection;

---

[1] Much like the "tiered access" model proposed in the Expert Working Group's *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*, p. 86, https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

[2] https://tools.ietf.org/html/draft-lozano-tmch-func-spec-10

[3] Id. At 21, table of use cases in EWG report

- digital forensics and incident response;
- email and data security; and
- protection from spear-phishing and malware, botnets, DDOS attacks.

To become accredited, entities should:

1. be able to provide:
    a. Verifiable credentials; and
    b. letters of authority/endorsement from governments, companies, and/or individuals on whose behalf they are authorized to act (e.g., hired to protect from security threats including but not limited to spam, malware, malicious apps, denial of service, ex-filtration of content, persistent threats, fraud and other harms).

2. be willing to agree to:
    a. the terms of service,
    b. prevent abuse of data accessed,
    c. be subject to de-accreditation if they are found to abuse use of data, and
    d. be subject to penalties

Examples include: Akamai, BAE Systems, Cloudflare, IBM Security, Sophos, Symantec.

2. Intellectual Property

This category is designed for intellectual property rights holders, including trademark, patent or copyright owners or their attorneys or agents (agents may include trade associations, data aggregators and brand protection companies). Applicants in this category must provide:

- evidence of ownership of intellectual property rights (e.g., a trademark registration); or
- letters of authorization from the rights holders to act on their behalf.

This category of user must also:

1. Agree to use the data for legitimate and lawful purposes
2. Further agree to:
    a. the terms of service;
    b. prevent abuse of data accessed; and
    c. be subject to de-accreditation if they are found to abuse use of data.

3. Non-governmental Public Safety and Health Organizations

Eligible entities include not-for-profit organizations that seek to protect public safety and health. Their legitimate and legal purposes include:

- Academic and other non-profits with a legitimate or legal purpose

- Child protection and child anti-abuse organizations
- Combating human trafficking
- Combating counterfeit pharmaceuticals
- Combating dangerous counterfeit products
- Combating hate, racism and discrimination

Applicants in this category must provide evidence of their:

- formation and mission
- activity to fulfill mission

This category of user must also:

1. Agree to use the data for legitimate and lawful purposes
2. Further agree to:
    a. the terms of service,
    b. prevent abuse of data accessed,
    c. be subject to de-accreditation if they are found to abuse use of data, and
    d. be subject to penalties

Examples include The Internet Watch Foundation, NCMEC, LegitScript, The Southern Poverty Law Center, the Anti-defamation League.

Legitimate and Lawful Purposes

This section contains a list of legitimate and lawful purposes for the above accredited Eligible Entities. Each purpose is mapped to an entity type.

Legal Actions

- Investigate fraudulent use of registrant's name by any other domain names
- Contact a registrant's legal representative
- Take legal action

Intellectual Property Enforcement

- Investigate possible intellectual property infringement
- Contact infringing parties
- Research a domain name's historical record
- Identify other domains registered with a given name or address
- Initiate or facilitate administrative proceedings

Security / DNS Abuse Mitigation

- Track and predict malicious behavior
- Investigate security and abuse trends
- Contact victims with compromised domain names
- Enable domain name white/black list analysis by security/reputation service providers

Regulatory and Contractual Enforcement

- Contractual compliance investigation
- Registration data escrow audits

Domain Name Administration

- Transfers of a domain between registrars or registrants

Public Health and Safety

- Gather evidence of activity dangerous to public health or safety
- Identify other domains registered with a given name or address that may be involved in activity that threatens public health or safety
- Report to government agency or law enforcement

Purpose and Entity Mapping[4]

Purpose	Entity - Reason
Legal Actions	● Security - To investigate/remediate fraud ● IP - To investigate/remediate infringement
Intellectual Property Enforcement	● IP - To investigate/remediate infringement, fraud, cybercrime
Security / DNS Abuse Mitigation	● Security/IP - To investigate/remediate and block criminal activity, fraud, technical exploits
Applicable Law, Regulatory and Contractual Enforcement	● Private Sector IP and Security - for investigation of crimes and DNS abuse for the purpose of protecting users from fraud and assembling data for Law Enforcement Agency response
Domain Name Administration	● IP - To administer domains ● Others - Contracted party usage not in scope, but they and others may need access to ensure chain of custody/ownership of domains for transfers and transactions.

[4] See also EWG report p.21

Certification Process[5]

All Eligible Entities must:

1) Submit an application with verifiable
   → contact details
   1. Name
   2. If Applicant is an agent, the name of individual or entity for whom agency exists
   3. Physical Address
   4. E-mail Address
   5. Telephone number
2) and required documentation
   → Cybersecurity & OpSec Investigators: Verifiable credentials and letters of authority
   → Intellectual Property: Evidence of IP ownership or a letter of authorization from the rights holder to act on its behalf

3) undergo validation by an ICANN approved agent (like the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse)

Once the Eligible Entity successfully completes steps 1 and 2 above, the ICANN approved agent issues one of two decisions:

→ The applicant is issued user credentials or a certificate.

Or

→ Rejection of the application

*Any Eligible Entity that receives login credentials must go through annual reaccreditation.

Proposed Operating Model

The new models conceived and considered in the *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)* are not workable due to the distributed nature of Whois databases. Under those models, each contracted (registry or registrar) party operating a Whois database will need to govern access. No changes are proposed to the existing Whois infrastructure other than creating gated access for individual record or automated access of Whois records including non-public elements. Collection, storage, and copy models are unaltered; however, authorization and access[6] changes are necessary.

[5] Note additionals scenarios for accreditation in Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 63,

[6] Note Models Considered, Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 110

Accreditation & Access Model
For Non-Public Whois Data
March 12, 2018
Version 1.1

In this proposed model, which is a federated model for access to Whois, eligible accredited entities can present their credentials to any Whois system. Contracted parties collect credentials, which are validated by a central authority, and the requesting entity is either granted or denied access to data.

Accredited Users

Upon accreditation, users are given credentials to access Whois data. . Users are able to present their credentials to a Whois database operator who validates credentials with a federated, centralized access authority and then provide access to Whois data. Responses to single record queries should be delivered via browsers and automated access should be be delivered via port 43 .

Contracted Parties and Agents

Contracted Parties (registries and registrars) and agents will accept credentials and provide access to non-public data for accredited users. They will rely on a centralized access authority tovalidate user credentials and then provide or deny access. Users will then be able to issue single-record or bulk queries against the Whois databases.

Logging

All accredited entities and agents query activity will be logged. Logs will include accredited entity, purpose, query, and date,. Logs must be retained in a machine readable format. Logs must be kept up-to-date with each new query. In the event of an audit or claim of misuse, logs may be requested for examination by an accreditation service or dispute resolution provider. Logged data must substantiate that accredited users are using data for legitimate and legal purposes as detailed above. Each query must be mapped to a purpose that is applicable.

Audit

A third-party firm should randomly audit a small sample of query logs for compliance with terms and conditions funded by accreditation and renewal fees. Additionally, Whois database operators may, once annually and at their expense, demand an audit of any accredited entity. A Whois database operator's logs for access may be matched to an accredited entity's logs by a third-party to discern misuse/abuse. (see EWG report Accountability and Audit Principles[7]) Also, query logs should cite purposes of access, which must be tied to a legitimate and legal use case for each accredited users use case. Audits will be conducted by a third-party bonded company, and logs are to be delivered with identity of the log origin tokenized or anonymized so that the auditing organization cannot see and thus risk identifying methods of accredited party

Central Access Authority

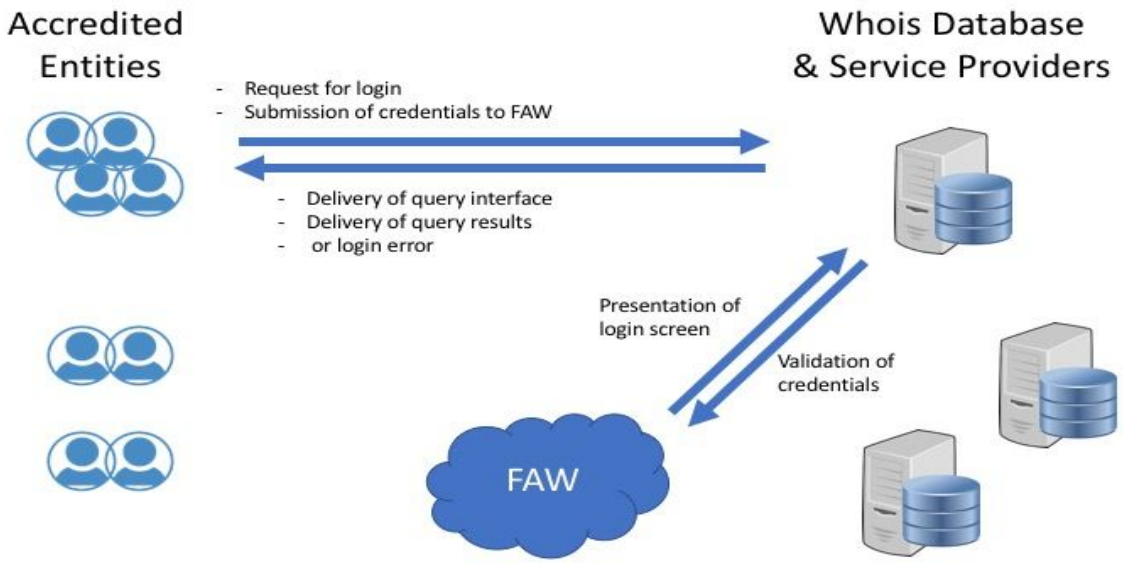
Login and authorization for access by accredited entities to Whois database operators at registries and registrars will be provided by a third-party or parties

[7] Note Audit Principles, Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 94,

Accreditation & Access Model
For Non-Public Whois Data
March 12, 2018
Version 1.1

Application and renewal fees should be sufficient to cover onboarding and support fees for the authorization and access system. Application and renewal fees should scale with the number of users for each accredited entity. Contracted Parties and Agents should need minimal support to integrate this authorization system into their workflow for gated access.Support for integration at contracted parties should come at no cost and be fee-based for agents.

Federated Access for Whois Diagram



Complaints

- Complaints regarding accuracy of data will be addressed directly to the domain name's sponsoring registrar for resolution.
- Complaints regarding performance of underlying WHOIS providers will be directed to ICANN compliance, who will address the matter with the appropriate registrar, according to the terms of the Registrar Accreditation Agreement.
- All other available remedies (e.g., filing false WHOIS complaints) are available to all appropriate parties.
- Complaints regarding unauthorized access to or improper use of data will be addressed to the accrediting agency, who will have the authority to restrict or deny further access to WHOIS data.

Penalties

The accrediting agency will audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor.

Accreditation & Access Model
For Non-Public Whois Data
March 12, 2018
Version 1.1

Different terms and conditions could be applied to different purposes. Violation of terms and conditions may result in graduating penalties, including but not limited to:

- Restricted or throttled access
- Denial of further access
- Financial penalties

Terms of Accreditation

Data Protection

Accredited users must protect the personal data in their custody queried from Whois systems and adhere to applicable law for the handling of personal data. At a minimum, individual companies and users have a responsibility to protect data at rest by accessing it on machines that are protected by passwords and have adequate security facility. Similarly, agents have a responsibility to protect the data that they provide to others, and therefore must:

1) gate access to data via password
2) secure data at rest through encryption
3) secure data in transit through encryption
4) validate with each login that users have up-to-date accreditation for use of the data.

Application Fees

All applicants must pay a non-refundable application fee proportional to the cost of validating an application. Rejected applicants may re-apply up to two times, each time paying the fee. Fees are to be established by validation authority.

-

Data Access

Accredited data access is to be provided for legitimate uses either for single record queries or automated queries for analysis. Accredited access shall not be rate-limited or otherwise restricted except as needed to ensure operations; any accredited user may have access to all Whois records from any ICANN contracted party. Data may be stored by accredited users for analysis and collection of case data. Stored data must at a minimum be secured by password and encryption, and use of and access to data must conform with terms of service. As stated above, accredited users and organizations must protect the personal data in their custody queried from Whois systems and adhere to applicable law for the handling of personal data.

Data Misuse Penalties

In the event of breach of the terms and conditions, any legitimate user's right to access, retain or use data is suspended. Upon being notified of a breach, a user's access privileges are revoked and that user must delete any retained data and provide notice to the certifying body that the data has been deleted. Data misuse violations may be appealed to accrediting body

(see EWG report, RDS User Accreditation Principles[8]) and access may be reinstated at the discretion of that body.

Agents that provide data to other accredited users are responsible for denying access to formerly accredited users whose privileges have been revoked for their misuse. Agents are also responsible for validating that their users are accredited and maintain accreditation; they must provide access only to currently accredited users or they are subject to misuse penalties.

Data Misuse

Data is not to be misused in any manner by any party. Categories of misuse could include the following non-exhaustive examples:

- Non-legitimate purposes (e.g., registration data mining for spam/scams)
- Data revealed as a result of a security breach
- Provision or sale of data to non-accredited parties for any reason
- Use of data for a purpose that is inappropriate for the accredited user type.

[8] Note RDS User Accreditation Principles, Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 62