DRAFT ACCREDITATION AND ACCESS MODEL FOR NON-PUBLIC WHOIS DATA

VERSION 1.7

Draft Accreditation & Access Model
July 20, 2018
Version 1.7

I. Overview

Following the implementation of measures for compliance with the European Union's General Data Protection Regulation (GDPR), this document provides a framework for an accreditation and access model (AAM) to provide access to non-public WHOIS data for legitimate and lawful purposes.[1] The initial draft of this model was based on the "tiered access" structure proposed by the Expert Working Group's Final Report.[2]

There is widespread recognition in the ICANN and regulatory communities of the need for development of an access model based on legitimate purposes. In its April 11, 2018 letter, the European Union's Article 29 Working Party (now titled the European Data Protection Board (EDPB)) noted that it:

> *…expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders…of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data. In this respect the WP29 encourages ICANN to develop appropriate policies and procedures applicable to incidental and systematic requests for access to WHOIS data…*[3]

In addition to the EDPB, governments, law enforcement, businesses, intellectual property owners and Internet users worldwide have expressed concern over WHOIS data outages and support for legitimate purpose access. On three occasions to date, ICANN's own Governmental Advisory Committee (GAC) has given consensus advice to the ICANN Board that ICANN should maintain WHOIS to the fullest extent possible and to mandate an access mechanism to non-public WHOIS data.[4][5][6] ICANN's Security and Stability Advisory Committee (SSAC), the ICANN Board's panel of experts on the technical integrity of the DNS, advised that degradation of the system's health is already taking place due to lack of access to registration data.[7] This view is also held by the Intellectual Property Constituency, the Business Constituency, and the At-Large Advisory Committee within ICANN, as well as other global entities and sectors outside of the ICANN community.

Building on ICANN Org's recognition of legitimate bases for the continued collection of full thick WHOIS data by registrars and registries, this accreditation and access model presents an available solution to the problem of access to non-public data elements while respecting the imperative of data privacy and complying with GDPR. Under this model, defined groups of organizations or categories of organizations can gain access to gated data if they (1) require access to data for specific, legitimate and lawful purposes (see Annexes B and K), and (2) are properly validated by a third-party accreditor.

Note that this model does not include provisions for law enforcement agencies (LEAs) and other governmental access, which is extremely important but is being separately addressed by governmental representatives. To the extent that governments wish to adopt elements of this criteria and adapt them for LEA accreditation, that would be welcomed, as would further collaboration and consultation between government and private sector representatives.

The ICANN community of participants is working to complete this model and seeks the most efficient avenue as possible for its implementation.

---

[1] Such access to data to be compliant with all facets of GDPR and any interpretations by data protection authorities and relevant bodies.
[2] Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), at p. 86
[3] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf
[4] https://gac.icann.org/contentMigrated/icann60-abu-dhabi-communique
[5] https://gac.icann.org/contentMigrated/icann61-san-juan-communique
[6] https://gac.icann.org/contentMigrated/icann62-panama-communique
[7] https://www.icann.org/en/system/files/files/sac-101-en.pdf

II. Framing the model according to ICANN's Q&A

This section sets forth answers regarding the AAM according to the questions posed by ICANN in its discussion paper of 18 June 2018, which broaches the subject of accreditation and access.

Eligibility

1. Who would be eligible for continued access for WHOIS data via the AAM?

Registrars would continue to be required to provide reasonable access to third parties on the basis of a legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject.

The AAM detailed here envisions access granted to various eligible entities that include, but are not limited to:

- Cybersecurity and OpSec Investigators
- Intellectual Property Owners and Agents
- Public Safety and Health Organizations
- Verification and Compliance Authorities

Note that the oft-cited law enforcement agencies are not listed here, as policy work is proceeding elsewhere in the community with regard to access for these authorities.

The eligible entities highlighted in Section III were initially derived from the list of entities and use cases documented in the EWG Report[8] and have evolved as a result of community feedback, but this is by no means an exhaustive list.

2. Who would determine eligibility under the AAM?

Eligible entities are those with legitimate purposes for access to non-public WHOIS data, in compliance with GDPR. Final determination of eligibility is made by an ICANN-approved accreditation review authority.

3. How would authentication requirements for legitimate users be developed under the AAM?

Accreditation would be provided by an ICANN-approved accreditation review authority. The accreditation authority would publish the criteria for access, which would encompass the three accreditation categories:

- Regular Access Accreditation
- Special Access Accreditation
- One-Time Accreditation

These categories are explained more fully in Annex G.

[8] At p.21. See table of use cases in EWG report.

Process Details

4. Who would be required to provide access to non-public WHOIS data under the AAM?

Registrars are required to provide access under the AAM.

5. What would be the overall process for authenticating legitimate users for access to non-public WHOIS data under the AAM?

Users are to be vetted by the accreditation authority based on credentials presented. Contracted parties are not expected to perform vetting.

All eligible entities must:

- Have a specific and delineated purpose for their access to and use of non-public data
- Certify that access to and use of non-public data is for a legitimate and lawful purpose and limited to the purpose for which it is sought.
- Affirm that they will not intentionally misuse the non-public data entrusted to them
- Comply with applicable laws (e.g., GDPR) and terms of service to prevent abuse of data accessed
- Be subject to de-accreditation if they are found to abuse use of data
- Be subject to penalties under applicable laws (e.g., GDPR)
- Submit an application with verifiable contact details:
    - Name
    - If Applicant is an agent, the name of the individual or entity for whom agency exists
    - Physical address
    - E-mail address
    - Telephone number
- Submit required documentation as covered more fully in Annexes C, D, E, F and G
- Undergo validation by an ICANN-approved agent (similar to the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse) as covered more fully in Annexes C, D, E, F and G.

Once the eligible entity successfully completes the above steps, the ICANN-approved accreditation authority issues one of two decisions:

Application is accepted and the applicant is issued credential
- Or –
Applicant is returned with questions
- Or –
Application is rejected

Accredited parties must renew their accreditation annually. Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority. User fees are due and payable upon the date of start of service, again on date of renewal, and with further access conditioned upon successful payment. Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation. The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

6. What scope of data would be available to authenticated users under the AAM?

Users would be granted access to the full WHOIS record for each query.

7. Would registry operators and registrars be required to provide access to non-public WHOIS data to all authenticated users under the AAM?

Registry operators and registrars would be required to provide global access to authenticated users consistent with the identified legitimate purpose, and subject to applicable local laws.

8. Would the AAM incorporate transparency requirements?

Accreditations for eligible entities will be subject to periodic review to ensure they meet the access purpose criteria. Logging should allow analysis of access to non-public WHOIS data to enable detection and mitigation of abuses and imposition of penalties and other remedies for inappropriate use. Appeal mechanisms will be available in the instance that a review results in de-accreditation.

9. Would there be any fees as part of the AAM?

All applicants must pay a to-be-determined 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 the accreditation authority.

Accredited parties must renew their accreditation annually. Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority. User fees are due and payable upon the date of renewal, with further access conditioned upon successful payment.

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.

10. Would there be a process to review the effectiveness of the AAM?

The contemplated review process would take place on the two-year anniversary of the launch of the accreditation program, then every five years following.

Technical Details

11. Would there be a central repository of WHOIS data from which access would be granted to authenticated users under the AAM?

The system is envisaged to:

a. Leverage and extend the existing ICANN centralized WHOIS system (as hosted on the ICANN website here). Contracted parties provide ICANN with full access to non-public WHOIS data via both RDAP and Port 43. Credentialed users submit individual queries from their whitelisted IP address(es) to the ICANN query mechanism and are granted access to individual non-public WHOIS records. (Note that whitelisting IP addresses as an access mechanism is applicable only to Port 43 access.)

b. Leverage and extend existing web-based access provided by contracted parties. Contracted parties provide credentialed users the ability to submit individual queries from their whitelisted IP address(es) to their web-based form and grant access to individual non-public WHOIS records.

12. What technical method would be required to provide access to non-public WHOIS data under the AAM?

Registry operators and registrars would be required to provide access to non-public WHOIS data via a Registration Data Access Protocol (RDAP) service.

13. What technical method would be used to authenticate users under the AAM?

As efforts to implement RDAP or the new RDS emerge, the methods for access to non-public WHOIS data for lawful and legitimate purposes may also evolve.[9] Two examples of this are as follows:

a. RDAP Open ID Connect Profile

Annex I defines a profile of the technical and operational requirements needed to support the identity, authentication and authorization mechanisms specified in draft-hollenbeck-regext-rdap-openid-07, describing a federated authentication system for RDAP based on OpenID Connect (OIDC). This method is available today.

b. Registration Directory Service Accreditation Authority ("RDSAA")

RDSAA could be used for Transport Layer Security (TLS) client authentication in conjunction with the RDAP. The high-level requirements for the RDSAA -- that will require an accreditation authority that issues public key certificates to those who seek access to the full non-public WHOIS data -- can be found in Annex J.

Codes of Conduct for Accessing Non-Public WHOIS Data[10]

14. What would be the role of Codes of Conduct in the AAM?

15. Would there be multiple Codes of Conduct?

16. How would the Codes of Conduct be developed?

17. What types of safeguards would be included in the Codes of Conduct?

18. What mechanism would be used to require compliance with the Codes of Conduct?

19. Who would monitor and enforce compliance with the Code of Conduct?

[9] Future updates could also include an anonymized or "tokenized" system whereby a data processor anonymizes data fields containing personal information -- replacing that information with consistent tokens across all WHOIS records in all WHOIS databases so that queries issued by accredited bodies can detect patterns of abuse without having access to the broad base of personalized data and need only then request reveals of personal data directly related to tokens triggered by the purpose of their search.

[10] NOTE: The authors have not (yet) formulated Codes of Conduct specifically for this model but note that the substance of this model contains elements that could become the basis for codes of conduct.

III. Eligible Entitles: Purposes and Eligibility Requirements

An eligible entity, for the purposes of this AAM, is a party that is entitled to registration data access. The entities listed here have legitimate and lawful purposes to access data, as do agents that facilitate protection of public interests, security and lawful behavior.

A. Cybersecurity & OpSec Investigators

This category is designed for security companies, organizations that need to protect their own interests and agents/companies that act on their behalf. The eligible entities in this category are companies, or individuals at companies, who provide cybersecurity or operational security for their company or another organization, or provide it as a solution and/or service to other individuals, entities or end-users. Agents in this category are cybersecurity concerns, financial institutions, academic institutions and researchers, OpSec investigators, and threat intelligence providers who aggregate data for correlation.

Legitimate and lawful purposes for access:[11]

- Predicting, investigating, tracking and preventing malicious behavior
- Researching and investigating security and abuse trends
- Contacting victims with compromised domain names
- Enabling domain name white/black list analysis by relevant service providers
- Maintaining integrity, availability and continuity of online platforms
- Initiating or facilitating legal proceedings

Examples of services covered:

- Identity and access management
- Application security
- Fraud protection
- Bank and payment processors and their compliance providers
- Digital forensics and incident response
- Email and data security
- Protection from spear-phishing, malware, botnets, DDOS attacks and other abuses
- Protection for end-users by online platforms, such as browsers, search engines, and social media
- Security intelligence and analytics
- Ensuring continuity, integrity and availability of Internet infrastructures
- Domain risk scoring and blacklist / blocklist creation
- Fraud and theft protection
- Bank and payment processing and their compliance providers
- Ensuring security, integrity, and availability of Internet infrastructures
- Incident response; computer emergency response team (CERT)
- Identity and access management
- Application security
- Email and data security

[11] See Annex K.

- Protection from malware, phishing, botnets, DDOS attacks, network penetration, and other abuses
- Reputational risk scoring and blacklist / blocklist creation
- Protection of end-users by online platforms, such as browsers, search engines, and social media platforms
- Security intelligence, analytics, and research
- Licensed private investigators
- Digital forensics

This category of user must also agree to follow vetting and accreditation processes (see Section IV, Procedures).

Examples of entities in this category: ICANN, HSBC, JPCERFT/CC, REN-ISAC, Akamai, BAE Systems, Cloudflare, IBM Security, Sophos, Symantec, DomainTools, Spamhaus and security organizations within companies like Salesforce, Facebook, and Microsoft.

For more information, please see Annex C.

B. Intellectual Property Owners and Agents

This category is designed for intellectual property rights holders, (such as trademark, patent or copyright owners), or their agents (agents are legal representatives and/or brand intellectual property protection companies) who need to investigate and enforce against abuses of their intellectual property rights to prevent consumer confusion and resulting harm. It also applies to OpSec actors who address brand-based phishing, malware and other abuse that facilitates criminal theft, product counterfeiting, etc. It may also apply to entities who are seeking to establish intellectual property rights in good faith who seek to conduct intellectual property rights clearance or due diligence investigations. Eligible Entities in this category should be members in good standing of a body that imposes and monitors professional responsibility and ethical standards for membership (such as a national or state/provincial licensing organization, bar association, national or regional intellectual property office, or trade association), or should otherwise be able to demonstrate legitimate intellectual property rights or specific good faith efforts to establish such rights.

Legitimate and lawful purposes for access:[12]

- Investigating, tracking and preventing intellectual property infringement
- Researching and investigating intellectual property infringement trends
- Contacting infringing parties and relevant service providers
- Identifying domains to support IP enforcement
- Initiating or facilitating legal proceedings
- Maintaining intellectual property rights
- Performing intellectual property rights clearance or due diligence

Examples of investigation and enforcement activity:

- Preventing consumer confusion, theft and fraud and other crimes (e.g., counterfeiting) through infringement of trademarks
- Identifying domains and actors attempting phishing attacks on corporate employees or customers
- Preventing the unauthorized distribution of copyrighted material
- Identifying and responding to trademark related claims, such as infringement or cybersquatting
- Intellectual property rights clearance or due diligence
- IP evaluation and investigation

This category of user must also agree to follow vetting and accreditation processes (see Section IV, Procedures).

[12] See Annex K.

Examples of entities in this category: Intellectual property attorneys, in-house corporate counsel, agents/staff of attorneys, and corporate or brand-protection-focused registrars (e.g. MarkMonitor and CSC), individual intellectual property rights owners or licensees, or organizations or individuals performing good faith intellectual property rights clearance or due diligence.

For more information regarding proposed accreditation criteria for intellectual property rights holders or parties performing intellectual property rights clearance or due diligence, please see Annex D.

C. Public Safety and Health Organizations[13]

Eligible entities in this category are organizations that seek to protect public safety and health, or the organizations that support them. These are organizations which are formally organized under the applicable laws of the country in which the organization is based, and which have identified their missions (as specifically identified in their documents or organization, such as bylaws or articles of incorporation) as specifically encompassing one of the following: academic and other non-profits with legitimate or legal public safety or health purposes; child protection and child anti-abuse organizations; combating human trafficking; combating counterfeit pharmaceuticals; combating dangerous counterfeit products; and combating hate, racism and discrimination.

Legitimate and lawful purposes for access:[14]

- Investigating, tracking and preventing activity that is dangerous to public health or safety
- Researching and investigating trends related to public health or safety threats
- Contacting victims of activity that is dangerous to public health or safety
- Identifying domains that may be involved in activity that threatens public health or safety
- Providing reports related to public health or safety threats to a government agency or law enforcement
- Initiating or facilitating legal proceedings

Examples of categories that are addressed through investigation and enforcement of applicable law:

- Fraud
- Theft
- Child abuse
- Human trafficking
- Sale of dangerous and illegal goods and substances
- Hate, racism and discrimination
- Terrorism and threats to national security

This category of user must also agree to follow vetting and accreditation processes (see Section IV, Procedures).

Examples of entities in this category: The Internet Watch Foundation, NCMEC, LegitScript, The Southern Poverty Law Center, the Anti-defamation League, Human Rights Watch, Amnesty International, and the Red Cross.

For more information, please see Annex E.

[13] There are a range of non-governmental organizations which serve a public health and safety function. For the purposes of clarity and certainty, this section has focused specifically on organizations with a mission to combat threats to public safety.
[14] See Annex K.

D. Verification and Compliance by Private Parties, Companies and Service Providers

This category is designed for private parties, including companies, service providers and individuals who require access to WHOIS data in order to verify registration details, comply with legal obligations in the course of performing crucial tasks for private parties in the public interest.[15] In this context, the public interest includes ensuring the efficacy of business transactions, fraud avoidance, and contractual compliance. Eligible entities are persons who provide investigations, due diligence, and legal compliance services for their company or as agents on their behalf. Also included in this category are academics, legal professionals, accountants, journalists and others who need access to Whois data in the course of their work for legitimate and lawful purposes.

Under this category, legitimate and lawful purposes for access, *inter alia*, include:[16]

- Investigating fraudulent use of a domain name, of a registrant's name and/or other details in domain name registrations
- Investigating defamation, phishing, fraud, and other online abuse, and to determine the scope thereof
- Asset investigation and recovery in connection with civil disputes such as asset conversion, debts, and breaches of contract
- Locating a person for service of process in civil actions or other non-criminal legal procedures
- Identifying parties and non-parties in civil actions, proceedings, or potential actions or proceedings
- Identifying registrants in connection with the prosecution or defense of a civil action or other legal proceeding
- Performing contractual compliance and due diligence investigations
- Conducting registration data escrow audits and other regulatory and contractual audits
- Validating website and domain name ownership and eligibility to conduct commercial activity
- Validating ownership in domain name purchase/sales transactions, brokering and escrow services
- Validating the transfer of domain names between registrars and/or registrants
- Investigating domain names, including historical records of domain names, registered to the same registrant in connection with purchases, sales, bankruptcy and receiverships, mergers and acquisitions, and other contractual and legal purposes
- Conducting journalistic, public interest and academic research

Categories of business entities: Corporations, Law firms, paralegals, accountants, financial advisors, IP consultants, domain brokerages, bankruptcy trustees, private investigators, escrow services companies, IP holders, secondary domain name marketplaces, individuals with a demonstrated need as listed above.

Examples of business entities in these categories: Dentons, Norton Rose (law firms) Hilco Streambank, Berggren, Media Options, BrandIT, Marksmen (IP consultants and brokers), Deloitte, KPMG, EY, PWC (accounting and financial advisors), Lazard, Morgan Stanley, Goldman Sachs, Barclays (M&A), Investigative Group International and Kroll (investigators), Escrow.com (escrow service providers), Carnegie Mellon University (academic research), and Sedo and Afternic (secondary domain name marketplaces).

For more information, please see Annex F.

[15] Pursuant to Article 6(1)(e) of the GDPR, "processing shall be lawful only if and to the extent that…the processing is necessary for the performance of a task carried out in the public interest." See: https://gdpr-info.eu/art-6-gdpr/
[16] See Annex K.

IV. Procedures

A. Accreditation Procedure

The accreditation approach for this AAM encompasses three (3) types of "Accreditation Categories":

- Regular Access;
- Special Access; and
- One-Time Access.

Accreditation would be provided by an ICANN-approved accreditation authority. The authority would publish the criteria for access, which would encompass the three accreditation categories, which are explained more fully in Annex G.

B. Validation and Review of Access Purposes

Accreditations for eligible entities will be subject to periodic review to ensure they meet the access purpose criteria. As discussed further below (see Section IV(D), Logging), logging should allow analysis of access to non-public WHOIS data to enable detection and mitigation of abuses and imposition of penalties and other remedies for inappropriate use.[17] Appeal mechanisms will apply in the instance that a review results in de-accreditation.

C. Process for Vetting and Accreditation[18]

Users are to be vetted by the accreditation authority[19] based on credentials presented. Contracted parties are not expected to perform vetting.

All eligible entities must:

- Have a specific and delineated purpose for their access to and use of non-public data
- Certify that access to and use of non-public data is for a legitimate and lawful purpose and limited to the purpose for which it is sought.
- Affirm that they will not intentionally misuse the non-public data entrusted to them
- Comply with applicable laws (e.g., GDPR) and terms of service to prevent abuse of data accessed
- Be subject to de-accreditation if they are found to abuse use of data
- Be subject to penalties under applicable laws (e.g., GDPR)
- Submit an application with verifiable:
- Contact details
    - Name
    - If Applicant is an agent, the name of individual or entity for whom agency exists
    - Physical Address
    - E-mail Address
    - Telephone number
- Submit required documentation as covered more fully in Annexes C, D, E, F and G.
- Undergo validation by an ICANN-approved agent (similar to the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse) as covered more fully in Annexes C, D, E, F and G.

[17] Much like the "Purpose-Driven Access" model proposed in the EWG Report, p.10.
[18] Note additional scenarios for accreditation -- Id. at 63.
[19] This responsibility could fall to a trusted third party, similar to Deloitte administering the Trademark Clearinghouse, or to WIPO, an international independent and neutral organization.

Once the eligible entity successfully completes the above steps, the ICANN-approved accreditation authority issues one of two decisions:

Application is accepted and the applicant is issued credential
- Or –
Applicant is returned with questions
- Or –
Application is rejected

Accredited parties must renew their accreditation annually. Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority. User fees are due and payable upon the date of start of service, again on date of renewal, and with further access conditioned upon successful payment. Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation. The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

D. Proposed Operating Model & Temporary Access Protocol

i. Temporary Access Protocol

The operational aspect of the accreditation and access model proposed here is a pragmatic solution for interim compliance with GDPR and can be implemented quickly with minor modifications to existing systems. The proposed approach would allow gated access to non-public WHOIS data while achieving the goals of:

- Uninterrupted service
- Maintaining the pre-May 25th WHOIS system to the greatest extent possible
- Simplified and consistent implementation
- Centralized logging

Under this proposed approach, once accredited, access to WHOIS data should be administered by ICANN, who would be responsible for delivering to the contracted parties information regarding the accredited entities or individuals in a timely manner. More details can be found in Annex H.

ii. Permanent RDAP-based Solutions

As efforts to implement RDAP or the new RDS (through the RDS PDP process) emerge, the methods for access to non-public WHOIS data for lawful and legitimate purposes may also evolve.[20] Two examples of this are as follows.

a. RDAP Open ID Connect Profile

Annex I defines a profile of the technical and operational requirements needed to support the identity, authentication and authorization mechanisms specified in draft-hollenbeck-regext-rdap-openid-07, describing a federated authentication system for RDAP based on OpenID Connect (OIDC). This method is available today.

[20] Future updated could include an anonymized or "tokenized" system whereby a data processor anonymizes data fields containing personal information, replacing that information with consistent tokens across all WHOIS records in all WHOIS databases so that queries issued by accredited bodies can detect patterns of abuse without having access to the broad base of personalized data and need only then request reveals of personal data directly related to tokens triggered by the purpose of their search.

b. Registration Directory Service Accreditation Authority ("RDSAA")

RDSAA could be used for Transport Layer Security (TLS) client authentication in conjunction with the RDAP. The high-level requirements for the RDSAA -- that will require an accreditation authority that issues public key certificates to those who seek access to the full non-public WHOIS data -- can be found in Annex J.

E. Logging[21]

The query activity of all accredited entities will be logged by the entity that provides access to the WHOIS queries. Logs will include accredited entity, purpose, query, and date. Logs must be retained for a two-year period in a machine-readable format and be kept up-to-date with each new query. Logged data will remain confidential by default and can be revealed only under legal justifications (revelation could, for example, compromise law enforcement investigations). In the event of an audit or claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider. Logs should be further available to data protection authorities and ICANN for auditing. Each query must be mapped to a purpose that is applicable. These steps will allow for auditing of 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. Similar to what was proposed in the EWG Report, auditing will encourage accountability regarding use of gated data for designated purposes only.[22] Note that appropriate restrictions to logs should exist -- as the EWG Report stated: "Access to logs must be restricted to those trusted, authenticated, authorized individuals and entities with a specific purpose and 'need to know.' [including] (to monitor RDS compliance with data protection legislation.)."[23]

ICANN should require that the WHOIS server operators (registrars and registries) and the querying parties log the queries made under tiered access. Access controlled by IP allows WHOIS server operators to log exactly what approved party has queried what domain name in WHOIS, and to timestamp the queries. Those performing the queries also must log their usage, recording what domains they queried when, to what WHOIS servers, and for what purpose. This type of logging is straightforward to implement accurately. Some registrars already log by what WHOIS queries are made from what IP addresses for what specific domain names. All registry operators are already required by ICANN to log how many WHOIS queries they serve.

F. Abuse Reporting

The system will be suitably transparent to allow appropriate access to third party examination of query rate and volume. A mechanism will be provided for reporting to the accreditation authority over-extensive use, mirroring or other abuses, for the purpose of investigation and possible revocation of accreditation.

G. 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. A contracted party'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[24]). Also, query logs should cite purposes of access, which must be tied to a legitimate and legal use for each accredited

[21] Logging responsibility decisions must be deferred until the technical implementation of the WHOIS query mechanism is decided. If contracted parties receive queries, they will have responsibility. If using the ICANN centralized WHOIS, ICANN will be responsible.
[22] EWG Report, p.91.
[23] *Id.* at 116
[24] *Id.* at 94

user's 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 an accredited party. Audit scope may include a request for correspondence sent by accredited entities to registrants as a result of access and use of non-public WHOIS data to validate that access and use of non-public data was not for illegitimate purposes (e.g., spam).

H. Fees and Renewal

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.

I. 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's Compliance Department, which will address the matter with the appropriate registrar or registry operator, according to the terms of the contract.
- All other available remedies (e.g., filing data accuracy complaints) are available to all appropriate parties.
- Complaints regarding unauthorized access to, or improper use of, data will be relayed to the accrediting agency for appropriate remedial action (see following sections on Penalties and Data Misuse Penalties).

J. Penalties

An auditing agency will audit non-public 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.

Different terms and conditions are applied to different purposes. Violation of terms and conditions may result in graduated penalties (such as restricted/throttled access, or denial of further access -- see Section V(f), Data Misuse Penalties).

V. Terms of Accreditation

A. Data Protection

Binding terms must require that parties accessing non-public WHOIS data must put appropriate internal controls in place at their organizations. This should include technical security and policies to control the storage of the data, to control and limit access to the data, and to oversee the usage of the data per intended purposes. Further, binding terms must state that parties accessing non-public WHOIS data are subject to GDPR's data retention obligations.

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 acting on the behalf of companies or individuals who have legitimate use of the data have a responsibility to protect the data that they provide to others, and therefore must:

- Gate access to data via password
- Secure data at rest through encryption
- Secure data in transit through encryption
- Validate with each login that users have up-to-date accreditation for use of the data

B. 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 accreditation authority.

C. 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 full 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 and applicable law.

Per GDPR, any accredited user will be expected to only process the personal data that it actually needs to process in order to achieve its processing purposes. They will be obligated to minimize the number of queries they make.

D. Data Forwarding

It will not be permissible to forward data to another party (whether accredited or not) except as allowed under applicable law. Users will agree as such via the terms of use and/or any applicable code of conduct.

E. 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 (unless acting as an accredited agent)

- Use of data for a purpose that is inappropriate for the accredited user type

F. Data Misuse Penalties

In the event of breach of the terms and conditions, any accredited user's right to access, retain or use data may be suspended.[25] Upon being notified of a breach, a user's access privileges may be revoked, in which case that user must delete any retained data and provide notice to the auditing agency that the data has been deleted. Data misuse violations may be appealed to accrediting body (see EWG Report, RDS User Accreditation Principles[26]) and access may be reinstated at the discretion of that body.

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

[25] Further, depending on the nature of the misuse, GDPR penalties may apply.
[26] *Id.* at 62.

Annex A: Rationale

Domain name registration data is a vital tool for the safe and stable operation of the domain name system, the prevention of crime, the protection of consumers, and many other critical tasks.[27] This formerly open and available database, however, has been effectively shuttered since May 25, 2018, when GDPR came into effect.

In advance of and since that date, the domain name community has worked together to establish a model that will accredit various eligible entities for access to non-public WHOIS data in a manner that complies with the GDPR law. Much of that work is represented in this document.

Concurrent with the effective date of GDPR provisions, the ICANN Board imposed a temporary contractual specification that operationally limits public access to WHOIS data. This specification imposes upon registries and registrars a temporary GDPR compliance model, but without a mechanism for access to non-public WHOIS data for legal and legitimate purposes.

This has effectively disabled the important functions that WHOIS previously supported. The outage is a significant problem for many reasons, including:

- Bad actors operate at a global scale, across multiple registrars and top-level domains, sometimes using thousands of names in coordinated and automated attacks.
- Harms range from consumer fraud, disinformation, spam, and phishing, to the more grim, including human trafficking and child abuse.
- The harm inflicted is dangerous, disruptive and expensive, and prevention or remediation windows are often measured in seconds or minutes, not days or weeks. The consequences of inaction or impaired action can be disproportionate, dire and irreversible for Internet users worldwide.
- WHOIS data elements, which are collected in conjunction with a domain registration contract, are extraordinarily useful in preventing or in investigating and prosecuting against these harms. For example:
- Within WHOIS, a point-of-contact data element, or elements in combination, are often used to expand an investigation beyond a single abused domain to a larger set of jointly controlled and/or connected domains that are used to scale harms exponentially.
- Attribution is critical to minimizing false positives when attempting to discriminate between maliciously and legitimately registered domain names and host names.
- Automated access for a specific legitimate purpose enables surgical, proactive security blocking to prevent spam, phishing attacks, and other abuse from reaching consumers in the first instance.
- Moreover, ICANN org's model has impaired or prevented crucial legal verification, investigation, compliance, and rights enforcement obligations, which are critical to the protection of the public. For example:
- Companies, and their agents who perform due diligence, compliance, and verification in connection with the acquisition or disposition of assets, bankruptcies and receiverships, and related professional services, have had their ability to comply with obligations impaired or prevented.
- Consumers face fraud and domain name theft as a result of the inability of secondary domain name marketplaces and escrow services to verify and investigate domain name transfers and transactions, thereby increasing risk of greater instances of fraud, theft and identity theft.

[27] Historical information (see http://forum.icann.org/lists/gnso-dow123/docfMF1nFg7Zy.doc) affirms that WHOIS data is not meant to be constrained to use only in resolving technical issues, but "rather to allow any person to contact any other person who had obtained an online address, regardless of purpose."

Annex B: Purpose Statement for the Collection and Processing of WHOIS Data

The GDPR requires that the collection and processing of personal data be for "specified, explicit and legitimate purposes." (Article 5(1)(b). In addition to processing that is necessary for the performance of a contract to which the data subject—in this case a registrant—is party, the GDPR permits processing that is necessary for the public interest or the legitimate interests pursued by a third party. (Article 6)

The following purpose statement meets the requirements of the GDPR, is in line with the proposals of the EWG's final report[28] and ICANN's Cookbook,[29] and supports the public interest and expectation by individual users that the Internet be a safe and secure place by ensuring safety and security through accountability.

The Internet is a public resource governed by a set of private arrangements that replace a system that otherwise would be created by national and international laws. These private contracts, executed under the oversight of ICANN, come with responsibilities, to serve many public policy interests -- especially because (as seen in ICANN bylaws) ICANN's mandates go beyond the mere technical function of mapping names to numbers.

One of these contractual obligations is WHOIS. The WHOIS system plays a key role in accountability online and ICANN needs to adapt the current WHOIS system to comply with the GDPR in line with its new Bylaw commitments requiring that ICANN "use commercially reasonable efforts to enforce its policies relating to registration directory services and work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."

As such, in support of ICANN's mission to coordinate and ensure the stable and secure operation of the Internet's unique identifiers, personal data found in domain name registration data may be collected and processed for the following purposes:

1. Collect and process accurate domain name registration data in a manner designed to respect the domain name registrant's fundamental privacy rights (as applicable), and minimized to provide for administrative processing.
2. Require that gTLD registries and registrars to provide a way to allow the public to contact registrants.
3. Provide access to appropriate and purpose-limited registrant data for consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection, while respecting the registrant's privacy rights (as applicable), and assessing and balancing of interest of the requestor and the registrant rights as required by law
4. Provide access to appropriate registrant data for law enforcement needs, consistent with protection of privacy rights of the registrant (as applicable), and assessing and balancing of interests of the requestor and the registrant's rights as required by law
5. Facilitating the provision of zone files of gTLDs to Internet users;
6. Providing mechanisms for preserving domain name(s) registrations via data escrow storage and recovery in the event of a distressed registrant or failure of a registrar or registry to fulfill its obligations.
7. Coordinating dispute resolution services for certain disputes concerning domain names; and
8. Ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems through at a minimum, addressing contractual compliance

[28] *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*, p.16.
[29] The Cookbook, Section 7.2.1, at 34. https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf

functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation.

The following chart ties this purpose statement to the performance of the domain name registration contract between the registrar and the registrant, public interests and legitimate interests pursued by a third party:

Purpose	Objective	Basis/Interest	Processing	Indicative Users
Domain Name Initial Purchase/ Registration, Management and Control	Tasks within this purpose are creating, managing and monitoring a Registrant's domain name (DN), including creating the DN, updating information about the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and validating the Registrant's contact information (pursuant to RAA requirements).	Performing and satisfying contractual obligations	• Collection of the data; transfer of data to registry and escrow providers to ensure preservation of data • Inter-registrar transfers • Validation of Registrant data for accuracy • Validation for any restricted TLDs • Zone file provisioning • Storage for retention at least during registration term	Registrants, Registrars, Registry Operators, Escrow Providers, privacy proxy providers, ICANN
Business/Personal Domain Name Purchase or Sale	Tasks within this purpose are making purchase queries about a DN, transferring a DN to another Registrant, acquiring a DN from another Registrant, and enabling due diligence research by the purchaser to ensure that the DN is suitable for purchase and that the seller is bona fide. To accomplish these tasks, the user needs access to the Registrant's Organization and email address, and in some cases additional data – for example, to perform a Reverse Query on the name of a Registrant or contact to determine other domain names with which they are associated.	Prerequisite for functioning marketplace for domain names	• Validating Registrant email contacts for transfers • Contacting Registrant for potential sale • Performing reverse query on registrant information to ensure the sale will meet specific business criteria • Foregoing requires storage, publication and access of WHOIS data	Registrants, potential DN buyers, resale agents, Registrars
Technical Issue Resolution	Tasks within this purpose are working to resolve technical issues associated with DN use, including email delivery issues, DNS resolution failures, and website functional issues. To accomplish these tasks, the user needs the ability to contact technical staff	Providing security and stability of the DNS, consumer protection, and protection of Registrants expectation of service Providing a pathway for resolving technical problems/ issues	• Validation of Registrant information • Provision of access to technical users • Foregoing requires storage of access to technical contact information	Registries, Registrars (Network Operations); DNS service providers; cybersecurity experts

	responsible for handling these issues. (Note: It might be useful to designate multiple points of contact to address various kinds of issues – for example, postmaster for email issues.)			
Domain Name Certification	Tasks within this purpose are a Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name. Registrants seek certification to increase consumer trust and confidence in their website associated with the DN. To accomplish this task, the user needs to confirm that the DN is registered to the certificate subject; doing so requires access to full WHOIS data about the Registrant.	Protecting registrant's interest in maintaining secure DN Providing consumer protection and security	Validation of registrant contact info for EV, DV, OV SSL certifications -Foregoing requires storage of and access to full WHOIS data	Certificate Authorities, SSL Certification providers, Registrants, Registrars
Individual Internet User Protection Security and Trust	Tasks within this purpose are identifying the organization/service provider using a DN to instill consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them. To accomplish these tasks, the user needs the name of the organization/ service provider (preferably identity-validated) and its email address, and may benefit from following a contact URL to a page that describes the organization/service provider and its customer service contacts or allows the user to submit a customer service inquiry.	Safety, consumer trust and protection, validation of trustworthiness of the information provider.	• Validation of organization/service provider contact information • Provision of access to consumers and other third parties relying on services/information being provided by the organization/service provider • Foregoing requires storage and publication of and easy access to WHOIS data • Ensuring identity and organizational affiliation of websites conducting commercial activity like accepting credit card or other electronic payments or placing advertisements & promotions	Consumers, online platforms, and the general public
Academic/ Public Interest DNS Research	Tasks within this purpose are academic public interest research	Promotes broad range of research purposes to improve function, use	• Access to public data and certain	Students, research orgs, journalists, and academics

	studies about DN including public information about the Registrant, the domain name's history and status, and DNs registered by a given Registrant (Reverse Query). To accomplish these tasks, the user needs the ability to access all public data in the WHOIS directory and in some cases may need access to data for use in anonymized, aggregated form.	security, and stability of the DNS; Supports freedom of expression and academic research	non-public data in anonymized form. • Foregoing requires the storage, publication and access to WHOIS data	
Legal Actions	Tasks within this purpose are investigating possible fraudulent use of a Registrant's name or address by other registrants, investigating possible trademark infringement, fraud, copyright infringement, or other civil law violations, contacting Registrant or Registrant's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. To accomplish these tasks, the user needs the ability to contact the Registrant or its legal representative, without relay through an accredited Privacy/Proxy provider.	• Investigating and remediating possible IP infringement or other civil law violations • Preventing fraud and other forms of abuse • Facilitating the establishment, exercise, or defense of legal claims	• Disclose to third party rights owners; potential legal complainants • Facilitate identification of a response to fraudulent use of legitimate data (e.g. address) for domain names belonging to the same or other Registrant by using Reverse Query on identify-validated data. • Foregoing requires the storage, retention, publication and access to the full WHOIS data; enabling reverse WHOIS lookup	IP lawyers; intellectual property owners, brand protection and enforcement services companies and associations; cybersecurity experts; Registrars; Registry Operators
Regulatory and Contractual Enforcement	Tasks within this purpose are tax authority investigation	• Supports audit and enforcement of private and	• Storing and disclosing data to regulators, ICANN	Regulators, ICANN Compliance, Parties to contracts, Administrative and

	of businesses with online presence, UDRP or URS investigation, contractual compliance investigation, and registration data escrow audits. To accomplish this, user needs access to Registrant contact and DN data elements, such as email address and telephone number, as appropriate for the stated purpose. For example, ICANN approved domain name dispute resolution providers need access for domain name dispute resolution.	public legal obligations • Supports security, stability and trustworthiness of DNS	and authorities entrusted with domain name dispute adjudication. • Foregoing requires storage, retention and access to WHOIS data.	enforcement entities such as WIPO
Public Health and Safety Protection and Criminal Investigation	Tasks within this purpose are investigating and reporting threats to public health and safety, including reporting such threats to third party that can investigate and address that threat/abuse, derive investigative leads, serve legal process and/or contact entities associated with a domain name during a criminal investigation. To accomplish these tasks, the law enforcement agent, first responder, public health and safety organizations (e.g. Internet Watch Foundation) needs to quickly and reliably identify the Registrant and all other entities involved with this service provision / maintenance	Public health, safety and security Investigating cyber-crimes and cyber-enabled crimes;	• Detecting abuse by providing access to Registrant data for protecting public health and safety, including by accessing historic full WHOIS data for some period of time • Providing access to Registrant data for the purposes of detecting and mitigating criminal activity, including by accessing historic full WHOIS data for some period of time • Reporting abuse and potential criminal activity, including sharing WHOIS data among multiple public health and safety organizations, organizational and corporate digital crimes teams, law enforcement agencies in multiple jurisdictions to address cross-border nature of abuse/criminal	Law enforcement and government or private entities entrusted with enforcement responsibilities; public health and safety organizations, including victim advocacy organizations; digital crime/abuse teams.

			activity • Foregoing requires storage, retention and access to full WHOIS data; enabling reverse WHOIS lookup to determine breadth and scope of abuse and properly identify person/entity responsible for abuse and/or criminal activity.	
DNS Abuse Study, Investigation and Mitigation	Tasks within this purpose involve identifying the proliferation of malware, botnets, spam, phishing, identity theft, DN hijacking, data hacking, distributed denial of service attacks (DDOS), etc, and deploying mitigation measures to combat such abuses. Tasks in this purpose also are processes that security professionals use to defend their organizations' networks including risk assessing domains that trip alerts on their network (domains attempting to communicate with the network, or for example employees attempting to navigate to websites), as well as correlating WHOIS data with other network telemetry and contextual data they may have on these domains, pivoting from one domain to map resources controlled by active attackers, and if	• Protecting Registrant from abuse and hijacking of Registrant's DN • Consumer trust in the Internet • Ensuring network and information security and stability of the DNS • Combating unlawful or malicious/abusive actions negatively affecting secure and stable functioning of the DNS	• Providing access to Registrant data for the purposes of detecting and mitigating DNS abuse • Foregoing requires storage, retention, publication and access to WHOIS data; enabling reverse WHOIS lookup	Law enforcement and public safety agencies; Cybersecurity firms and individual cybersecurity analysts and experts; Online platforms Registry Operators, Registrars ICANN Compliance

	necessary driving to attribution of these attacks to the individuals and organizations behind them.			
ICANN DNS Oversight	Tasks within this purpose involve ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems, through at a minimum, addressing contractual compliance functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation.	• Promoting choice and competition and ensuring the stability, security, and resiliency of the DNS • Addressing contractual compliance obligations • Supporting audit and oversight functions	• Storing and disclosing data to ICANN • Foregoing requires storage, retention, publication and access to WHOIS data	ICANN organization

Annex C: Accreditation Approach for Cybersecurity & OpSec Investigators

The Anti-Phishing Working Group (APWG) will act as the designated accreditation authority that reviews the qualifications of applicants and maintains oversight of applicants for accreditation in this category. The APWG is a global not-for-profit research, educational, and industry association. APWG's mission is to aid response to cybercrime and cultivate responses to it through data exchange, research, and public awareness. The APWG operates cybercrime data exchanges, publishes cybercrime statistics, and presents international cybercrime conferences. It has more than 2,200 members worldwide, including Internet infrastructure and service providers, financial services companies, telecom providers, government CERTs, antivirus firms, and researchers. The APWG conducts its activities through a U.S.-incorporated non-profit 501(c)6.

APWG.EU is a chapter of the APWG, and was founded in 2013 as a Spanish non-profit scientific research foundation. APWG.EU's mission is to engage European businesses and organizations in the fight against identity theft and Internet-based crime. As part of this mission, APWG.EU organizes and presents at least one cyber-crime convention per year. The foundation is strictly not-for-profit, and is supported by grants, donations, and nominal membership fees.

Eligible Entities: Purposes & Eligibility Requirements[30]

In addition to previously listed eligible entities, entities in this category seeking accreditation must be an organization that fulfills a function related to the prevention, mitigation, and/or investigation of cybercrime. The organization may provide cybersecurity or operational security for itself or another organization, or may provide it as a solution and/or service to other individuals, entities, or end-users.

"Cybercrime" is defined as: "Acts that are committed against individuals or groups of individuals with a motive to intentionally cause loss, or physical or mental harm, or harm the reputation of the victim, directly or indirectly, using computers and/or modern telecommunication networks such as Internet and mobile phones." While criminal statues vary by jurisdiction, the acts of concern are generally considered deceptive, malicious, or criminal.

Examples of relevant functions:

- Identity and access management
- Application security
- Fraud protection
- Bank and payment processors and their compliance providers
- Digital forensics and incident response
- Email and data security
- Protection from spear-phishing, malware, botnets, DDOS attacks and other abuses
- Protection for end-users by online platforms, such as browsers, search engines, and social media
- Security intelligence and analytics
- Ensuring continuity, integrity and availability of Internet infrastructures
- Domain risk scoring and blacklist / blocklist creation
- Fraud and theft protection
- Bank and payment processing and their compliance providers
- Ensuring security, integrity, and availability of Internet infrastructures
- Incident response; computer emergency response team (CERT)

[30] APWG membership or cost recovery fee may be required.

- Identity and access management
- Application security
- Email and data security
- Protection from malware, phishing, botnets, DDOS attacks, network penetration, and other abuses
- Reputational risk scoring and blacklist / blocklist creation
- Protection of end-users by online platforms, such as browsers, search engines, and social media platforms
- Security intelligence, analytics, and research
- Licensed private investigators
- Digital forensics

Accreditation Procedure

The accreditation authority will provision a request for application to the APWG's Enrollment Manager, who then determines a candidate's eligibility for enrollment.

In addition to the information enumerated in Section IV, an accreditation application for this category will further require:

- Contact details
    - Name of applying organization
    - Name of applicant contacts
    - If Applicant is an agent, the name of individual or entity for whom agency exists
    - Physical Address
    - E-mail Address
    - Telephone number
    - Web site address
- Description of incorporated entity's functions/business
- Names and positions of all corporate officers and board members
- Copy of incorporation papers
- Statement of legitimate purpose(s) for access to non-public domain registration data
- List of primary staff members who will have access to the data
- Relevant licenses or professional certifications possessed by staff. (CISSP, government security clearances, private investigator license, etc.)
- Operational and data security arrangements:
    - Location where the data will be stored
    - IT and physical security for locations where data will be stored and accessed from, including the identification of any existing international or industry relevant security standards the applicant commits to.
    - Data access controls: policy for access, vetting of employees with access, etc.
    - Data retention policy
    - Data breach notification procedures to APWG and supervisory authorities

Responses will be reviewed and scored using an internal evaluation guide. The evaluator may seek clarifications regarding any incomplete or unclear responses.

Complete applications will then come before the APWG's Accreditation Review Panel, where the application material and evaluation will be presented. The panel will function according to an operational charter that describes its functions and procedures. These include:

- The Panel consists of five members with relevant professional backgrounds, such as in cybersecurity or privacy law.
- Members must fill out a disclosure of interests form that is shared with APWG Board and the other members of the Panel. Members expected to recuse themselves from discussions and decisions that may involve a conflict of interest.
- The Panel may avail itself of outside experts, such as to perform background checks.
- The Panel makes its decisions based majority vote.
- When the Panel reviews an application, it issues one of three decisions:
    - Application is accepted,
    - Application is returned with questions,
    - Application is rejected.
- The decisions of the Panel are final.

Once accredited, the accredited party will execute a contract with the APWG.

Once the contract is complete, the Panel will inform any necessary notifications or actions so that the accredited party can receive the access credentials that will allow it to make queries to the domain name registries and registrars.

Once credentials are issued, the accredited party may make queries as needed for legitimate purposes for as long as it remains accredited. Such need may be occasional or continuous/ongoing.

The Panel may perform audits of its accredited parties to review performance under the terms of the agreement.

The Panel will review complaints of misuse of access or data by the accredited parties and other violations of the terms of service.

Annex D: Accreditation Approach for Intellectual Property Owners and Agents

The following describes the criteria necessary to warrant accreditation for intellectual property owners and agents. The accreditation procedure follows that outlined in Annex G.

I. Accreditation Criteria

A. *Establishing Legitimate Interest in Protecting Intellectual Property Rights*[31]

1. **Trademarks**[32]

a. Registered Trademarks

i. Name of mark
ii. Registration number
iii. Registration date
iv. Jurisdiction
v. Description of goods and services class
vi. Detailed description of goods and services
vii. Status of the trademark holder (owner/assignee/licensee)
viii. Organization
ix. Full name
x. Address
xi. Contact information (phone, fax (if any), and email address)

b. Court Validated Marks[33]

i. Name of mark
ii. Reference number (number of the relevant court order)
iii. Decision date
iv. Jurisdiction
v. Name of court
vi. Court order (copy of or link to the order)
vii. Description of goods and services
viii. Status of the trademark holder (owner/assignee/licensee)
ix. Organization
x. Full name
xi. Address

[31] Intellectual property owners should only be required to be accredited on the basis of a representative sample of their intellectual property rights. A representative sample could be a minimum of three copyrighted works or trademarks, or fewer if the entity or individual owns fewer than three copyrighted works or trademarks. Ultimately, proof of at least one valid intellectual property right would be sufficient in all cases to accredit the requesting party, without the need for the party to be accredited separately for each individual intellectual property right they might own or be licensed to use.

[32] See TMCH Guidelines, v.1.2, Section 2.2.2 (Nov. 2013), available at http://trademark-clearinghouse.com/sites/default/files/files/downloads/TMCH%20guidelines%20v1.2_0.pdf (hereinafter "TMCH Guidelines").

[33] *See id.* Section 2.3.2

xii. Contact information (phone, fax (if any), and email address)

c. Marks Protected by Statute or Treaty[34]

i. Name of mark
ii. Reference number (number of the relevant statute or treaty)
iii. Date of protection (effective date of statute or treaty granting protection)
iv. Jurisdiction(s) where statute or treaty was enacted
v. Jurisdiction(s) where mark is protected by statute or treaty (if different from above)
vi. Title of statute or treaty
vii. Court order (copy of or link to the order)
viii. Description of goods and services
ix. Status of the trademark holder (owner/assignee/licensee)
x. Organization
xi. Full name
xii. Address
xiii. Contact information (phone, fax (if any), and email address)

d. Unregistered Trademarks

i. Name of mark
ii. Approximate date of first use
iii. Jurisdiction
iv. Description of goods and services
v. Description, specimen, or other evidence of use (only for unregistered marks, as rights are established by use in commerce)
vi. Status of the trademark holder (owner/assignee/licensee)
vii. Organization
viii. Full name
ix. Address
x. Contact information (phone, fax (if any), and email address)

If the party seeking to record the mark is a licensee of the mark owner, they should submit an applicable declaration that they are authorized users of the mark and provide evidence of same (e.g. a copy of an applicable license agreement).[35]

Further, if the trademark registration database in the jurisdiction where the mark has been registered is not publicly available online, the mark holder should also submit a copy of the applicable registration certificate.[36]

For trademark holders who have already recorded marks in the TMCH, they could simply use their existing TMCH record and/or Signed Mark Data (SMD) file to fulfill the trademark rights validation criteria.

Alternatively, trademark holders who have prevailed in UDRP or URS proceedings could use these determinations to fulfill the trademark rights validation criteria. These could be treated similarly to court-validated trademarks.

[34] *See id.* Section 2.4.2
[35] *See id.* Section 2.2.4
[36] *See id.*

2. **Copyrights**

a. Registered and Unregistered Copyrights

Where a legal entity is a member of a trade association comprised of companies which are in the business of owning significant numbers of copyrighted works, such as film studios or publishing and recording companies (e.g. the Motion Picture Association of America (MPAA), Recording Industry Association of America (RIAA), Association of American Publishers (AAP), Independent Film & Television Alliance (IFTA), or the International Federation of the Phonographic Industry (IFPI)), then evidence of membership in such a trade association is sufficient in order for the requesting party to receive accreditation. These trade associations themselves may also obtain accreditation where they demonstrate that they engage in intellectual property enforcement activities on behalf of their members, provided they sign a declaration that they are authorized to act on behalf of their members.

Alternatively, for entities or individuals that are not members of any such trade associations, they may obtain accreditation through submission of a declaration that they are a company engaged in the creation, production, and/or distribution of copyrighted works, by providing documentation and other materials as evidence to demonstrate their status, such as: company founding documents, advertising and/or marketing materials containing a description of copyright work(s), and identifying the owner of such works.

Alternatively, or in addition, an entity or individual can seek accreditation by submitting a representative sample of works as follows[37]:

i. Information reasonably sufficient to identify the copyrighted work, such as its title, owner, and/or year of creation
ii. Registration number (if applicable)
iii. Registration date (if applicable)
iv. Jurisdiction of creation (or registration if applicable)
v. Status of the copyright holder (owner/licensee)
vi. Organization
vii. Full name
viii. Address
ix. Contact information (phone, fax (if any), and email address)[38]

The preferred means of establishing copyright ownership is by way of showing evidence of registration of a copyrighted work. However, registration is not required for subsistence of copyright, and in some instances, there may be a delay between the time of a work's creation and its registration. Therefore, for unregistered works, the copyright holder may be required to submit additional evidence demonstrating valid copyrights in any work that is the subject of the accreditation request. This additional evidence may include: marketing materials containing a description of the work and identifying its owner, a redacted copy of a contract for publication or distribution of a work or similar contract, a copy of the copyright work or works (given content protection concerns, this would be at the discretion of the owner and could be subject to technological protections), prior court order(s) attesting to the ownership of the relevant copyright(s), any applicable copyright notices or publication announcements, or other evidence establishing the requestor's ownership of the copyrighted work. Such additional evidence should only be required in cases where there is a legitimate question as to the ownership of copyrights or agency by the party seeking accreditation on the basis of copyrights.

[37] A representative sample could be a minimum of three copyrighted works, or fewer if the entity or individual owns fewer than three copyrighted works.
[38] These criteria are based on the Draft Privacy & Proxy Accreditation Agreement Intellectual Property Disclosure Framework Specification, Sections 2.2.3-2.2.5 (version Feb. 28, 2018).

If the party seeking accreditation based on copyright is a licensee of the copyright owner, they should submit an applicable declaration that they are authorized licensees of the copyrighted work and provide evidence of same (e.g. a copy of an applicable license agreement).

3. **Other Intellectual Property Rights**

a. Geographical Indications and Appellations of Origin

i. Name of the Geographical Indication (GI) or Appellation of Origin (AO)
ii. Description of the goods or services that are protected
iii. Jurisdiction
iv. Nice Classification (if applicable)
v. Country of Origin or Production Area
vi. GI or AO Holder
vii. Status of holder (Entity - such as cooperative or association, Government office, other)
viii. Declaration from the competent authority granting rights in the Geographical Indication (IP Office or the competent national/regional authority in charge of GIs)
ix. Organization
x. Full name
xi. Address
xii. Contact information (phone, fax (if any), and email address

b. Designs

i. Name of protected design
ii. Registration number
iii. Registration date
iv. Jurisdiction
v. Description of protected design (abstract)
vi. Application Number
vii. Filing Date
viii. Detailed description of protected design (claims)
ix. Status of the design holder (owner/assignee/licensee)
x. Organization
xi. Full name
xii. Address
xiii. Contact information (phone, fax (if any), and email address)

c. Patents

i. Name of patented invention
ii. Registration number
iii. Registration date
iv. Jurisdiction
v. Status of the patent holder (owner/licensee)
vi. Organization
vii. Full name
viii. Address
ix. Contact information (phone, fax (if any), and email address)

d. Trade Secrets[39]

i. Description of the trade secret information
ii. Description of the economic value of the trade secret
iii. Description of efforts to maintain the secrecy or confidentiality of the trade secret information
iv. If trade secret validity has been determined by a court of competent jurisdiction:
a. Reference number of relevant court order (if any)
b. Decision date
c. Jurisdiction
d. Name of court
e. Court order (copy of or link to the order)
v. Organization
vi. Full name
vii. Address
viii. Contact information (phone, fax (if any), and email address)

e. Indigenous Intellectual Property Rights[40]

i. Description of the indigenous intellectual property, such as:

a. Cultural heritage
b. Traditional knowledge and traditional cultural expressions, and/or
c. Manifestations of sciences, technologies and cultures, including

i. human and genetic resources
ii. seeds
iii. medicines
iv. knowledge of the properties of fauna and flora
v. oral traditions
vi. literatures
vii. designs
viii. sports and traditional games
ix. visual and performing arts

[39] Trade secrets are a protected form of intellectual or industrial property within the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), available at https://www.wto.org/english/docs_e/legal_e/27-trips.pdf. *See* TRIPS, art. 39.
[40] Indigenous intellectual property rights are a protected form of intellectual property within the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), available at http://www.un.org/esa/socdev/unpfii/documents/DRIPS_en.pdf. *See* UNDRIP, art. 31.

ii. If the claimed indigenous intellectual property rights' validity has been determined by a court of competent jurisdiction:

a. Reference number of relevant court order (if any)
b. Decision date
c. Jurisdiction
d. Name of court
e. Court order (copy of or link to the order)
iii. Organization
iv. Full name
v. Address
vi. Contact information (phone, fax (if any), and email address)

B. *Intellectual Property Clearance and Due Diligence*

In addition to the legitimate purpose of protecting and enforcing existing intellectual property rights, there is also a separate but related legitimate purpose of performing intellectual property clearance and due diligence, in order to avoid infringing upon existing third-party rights. WHOIS data is often used in connection with this kind of effort,[41] so it would be necessary to establish an accreditation process for parties who may not yet own intellectual property rights but are performing due diligence as part of an effort to create a new intellectual property right without infringing on any existing rights.

In such cases, the party seeking accreditation should submit the following information:

1. Name of proposed trademark, copyrighted work, or other intellectual property right being evaluated
2. Description of the relevant intended mark, work, or other intellectual property right
3. Jurisdiction(s) where clearance and/or protection is sought
4. Organization
5. Full name
6. Address
7. Contact information (phone, fax (if any), and email address)

The requestor would need to submit some evidence demonstrating efforts to identify or develop the proposed intellectual property right, and evidence of other efforts to perform due diligence and clearance regarding same, which shall be kept confidential and not disclosed to any third party, including the subject of any data request, unless authorized by the requestor. The party requesting accreditation may also have an interest in keeping the request for data confidential, such as where there are binding confidentiality obligations or for other strategic reasons which dictate that such diligence efforts pursuant to any particular transaction not be disclosed to third parties.

[41] See, e.g., ICANN, gTLD Registration Dataflow Matrix (Oct. 13, 2017), available at https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-responses-redacted-13oct17-en.xlsx

Annex E: Accreditation Approach for Public Safety and Health Organizations

PLACEHOLDER WHILE THIS COMMUNITY ORGANIZES ITS INPUT REGARDING CREDENTIALING

Annex F: Accreditation Approach for Verification and Compliance by Private Parties

Where an individual or entity applies for accreditation and access under this category, in addition to satisfying the general requirements for accreditation and the requirements for the particular type of access requested by the applicant (i.e. Regular, Special, or One-time access) as set out below, the applicant will also be required to specifically identify itself and the nature of its legitimate and lawful purposes for which Whois data is required.

This will be accomplished by the applicant;

a) identifying themselves by 'type of entity or individual' under an enumerated category; and

b) correlating it with a particular legitimate and lawful use under one or more enumerated categories.

The below chart indicates the established enumerated types of potential appropriate applicants and the established enumerated types of potential legitimate and lawful uses for Whois data. An applicant will thereby identify themselves and one or more legitimate and lawful use, as may be applicable.

Type of Applicant Entity or Individual *(Select one)*	✓	**Type of Legitimate and Lawful Use** *(select one or more as may be applicable)*	✓
In-house counsel		Validating website and domain name ownership to ensure transparency and accountability for commercial activity and transactions;	
Law firm		Conducting forensic portfolio audits, domain name portfolio appraisals	
Paralegal		Validating chain of title to domain names that are the subject of a transaction or civil disputes	
IP Consultants and Domain Name Brokerages		Investigating and reporting on fraudulent uses of domain names and online abuse	
Accounting firm		Asset location and recovery	
Bankruptcy Trustee/Receiver		Initiating or responding to a legal proceeding and investigation thereof	
Financial Advisory firm		Providing escrow services for domain names and ensuring lawful and compliance transfers	

Secondary Domain Name Marketplaces		Transferring domain names between registrars or registrants	
Domain Name Escrow and Transfer Services		Academic research	
Auction House		Ascertaining legitimacy of website businesses	
Journalist		Public interest investigations	
Private Investigator		Broker and legal due diligence including chain of title examination via historical Whois records	
Academic Researcher		News reporting	
Internet User		Verifying if a website or email sender is trustworthy for commercial or other purposes	
Service Provider		Validating the ownership of website and/or domain name for SSL certificate acquisition and issuance, search engines or third parties performance monitoring	
Other		Retrieving the credentials used to register a domain, for instance when a domain was initially registered via a service provider or an employee, thus confirming that the registration was not fraudulent.	
		Other	

The applicant will also be required to submit a Certified Statement satisfactorily explaining;

a) the basis for the legitimate and lawful use;

b) why the accessed data is required;

c) what the accessed data will be used for; and

d) when the accessed data will be used.

It is anticipated that as the accreditation authority becomes familiar with the types of applicants and the applicants' typical basis for claimed legitimate and lawful use, that reviewing and processing the applications will become easier as most applications will follow the same or similar types and will therefore be easier to assess on an expedited and efficient basis.

As part of the application process, the applicant will be provided with standardized language setting out permissible explanations for the legitimate and lawful uses to reference in its application, so as to enable an expedited and efficient review of the application.

Where an application is an unusual in terms of either the type of applicant or the nature of the claimed legitimate and lawful purpose and/or does not follow the standardized and enumerated categories, the review and assessment of the application may involve a more involved review due to the particular and unique circumstances.

Annex G: Oversight of and Types of Accreditation

Oversight of Accreditation

Under this AAM, the accreditation authority bears the ultimate responsibility for granting accreditation to those with legitimate purposes for seeking registration data. However, recognizing that the authority may not have expertise in the subject matter of each category, it is envisioned that the authority plays an "oversight" role, while assigning evaluation of applied-for accreditation to sub-panels as necessary (for example, refer to the APWG's evaluation role for cybersecurity category accreditation in Annex C).

Types of Accreditation

A. Regular Access Accreditation

Regular Access Accreditation is for demonstrably trustworthy and secure companies who require access to the non-public WHOIS for a legitimate purpose on an ongoing and regular basis. For example, Escrow.com (a major escrow service provider) and Sedo (a major domain name marketplace) require access to WHOIS in order to validate a multitude of registrant identifications and to confirm a multitude of successful domain name transfers on a daily basis, pursuant to their respective legal obligations and duties to clients.

The evaluation of an applicant for Regular Access Accreditation would involve, *inter alia*, a rigorous inspection and evaluation of;

- its identity and supporting documents such as Articles of Incorporation, licenses, regulatory, and governmental filings;
- letters of references from credible sources familiar with the legitimate purposes and reputation of the applicant;
- a thorough and detailed description of its business, identification of the officers, directors, and shareholders, financial summaries or statements; and
- a detailed request setting out the basis for the legitimate purpose being claimed.

The accreditation authority would make a determination as to whether the applicant qualified based upon its level of ascertainable trustworthiness:

- financial stability;
- reputation;
- length of its establishment;
- qualifications of management and procedures for compliance and governance; and other factors which identify the applicant as an entity qualified and deserving of Accreditation; and
- other factors which identify the applicant as an entity qualified and deserving of Accreditation

The overriding criteria however, would be that the applicant has an established and credible legitimate purpose for requiring ongoing and regular access.

Applicants for Regular Access Accreditation would be required to post a bond to secure their obligations.

B. Special Access Accreditation

Special Access Accreditation is for those persons who require access to the non-public WHOIS database on an ongoing but intermittent basis for legitimate purposes. For example, the law firm, Norton Rose, would apply for Special Access Accreditation because it would anticipate that its lawyers would indefinitely require access in order to conduct due diligence, civil investigations, and for non-IP related civil actions, in connection with a wide variety of clients and matters which would not necessarily be known at the particular time of application for Special Access Accreditation.

The evaluation of an applicant for Special Access Accreditation would involve:

- inspection of its identity and supporting documents such as Articles of Incorporation, licenses, Law Society or Bar admissions, accounting licenses, and/or regulatory and governmental filings;
- licenses letters of references;
- a description of its business;
- identification of its officers, directors, shareholders, partners, or other ownership structure;
- a detailed request setting out the basis for the legitimate purpose being claimed; and
- The accreditation authority would make a determination as to whether the applicant qualified based upon;
- its level of ascertainable trustworthiness:
    - reputation;
    - length of its establishment;
    - qualifications of management and personnel;
    - procedures for compliance and governance; and
    - other factors which identify the applicant as an entity qualified and deserving of accreditation. The overriding criteria however, would be that the applicant has an established and credible legitimate purpose for requiring ongoing and regular access.

Special Access Accreditation alone however, would not enable access to the non-public WHOIS database. Rather, it would merely qualify the accredited party to make subsequent and expedited “Specific Access Requests”.

Specific Access Requests would be made to an administrative department of the accreditation authority which would evaluate each Specific Access Requests on a case-by-case basis, governed by specific criteria based upon identified legitimate purposes.

Because the recipient of Special Access Accreditation would have already been vetted by the accreditation authority, it is expected that such Special Access Requests would be evaluated and approved or denied on an instant, same-day, or expedited basis. Special Access Requests would need to identify the specific legitimate purpose of the request, such as to investigate specified claims of online abuse and defamation resulting from a particular website associated with a particular domain name.

C. One-Time Accreditation

One-Time Accreditation is for those persons who require access to the non-public WHOIS on an ad hoc or one-time basis for a specific and limited legitimate purpose. This could for example, include a law firm who has not applied or obtained Special Accreditation. It could also for example, include a researcher, investigator, journalist, or individual Internet user who is able to establish a specific legitimate purpose for one-time access for a specific reason.

Applicants for One-Time Accreditation would provide the following as part of their application to the accreditation authority:

- Notarized government issues photo identification;
- A detailed description of the basis for the request for one-time access, together with supporting documentation; and
- Any credentials, licenses, or other documents supporting the specific requirements and qualifications of the applicant.

Procedures

A. Certifications, Declarations and Obligations of Accredited Parties

The approval of accreditation will be contingent upon each applicant *inter alia*, agreeing to the following conditions:

- All information provided in the application for Accreditation is certified as true and correct;
- WHOIS access will only be used for the accredited and approved purposes and for no other purpose;
- All WHOIS data obtained through Accreditation will be kept confidential and not published, transmitted, or shared in any way, unless the applicant has obtained specific permission from the accreditation authority or the data is being provided to the client on whose behalf the services are being performed, as disclosed in the Accreditation application;
- All WHOIS data obtained through Accreditation will be subject to the data protection and security requirements specified by the accreditation authority;
- Comply with all applicable laws and regulations, as well as any policies set forth by ICANN or the accreditation authority; and

B. Validation and Review of Access Purposes

Accreditations for eligible entities will be subject to periodic review to ensure they meet the access purpose criteria. As discussed further below (see Logging), logging should allow analysis of access to non-public WHOIS data to enable detection and mitigation of abuses and imposition of penalties and other remedies for inappropriate use.

Accredited parties must renew their accreditation annually. Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority. User fees are due and payable upon the date of renewal, with further access conditioned upon successful payment. Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation. The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

C. De-Accreditation

De-Accreditation will occur when the accreditation authority determines that the Accredited person has materially breached the conditions of its Accreditation based upon either; a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Review Panel; or c) otherwise for any misuse or abuse of the privileges afforded. De-accreditation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Review Panel. De-accreditation procedures will be on reasonable notice to the Accredited person who shall have the right to a hearing and of appeal.

In the case of Regular Access Accredited parties, in the case of de-Accreditation, any posted bond may be forfeited in whole or in part, and other additional financial penalties may be assessed.

Accreditation Chart

Accreditation Category	**Type of Access**	**Accreditation Provider**
Regular Access	Ongoing access based upon initial approval of application for Accreditation	ICANN Accreditation Authority
Special Access	Once Accredited, must submit and obtain approval for Specific Access Request on each occasion where access is required	ICANN Accreditation Authority for initial application, followed by administrative department of Accreditation Review Panel for Specific Access Requests
One Time Access	Access permitted only on a one-time basis based upon a specific application for access	ICANN Accreditation Authority

Annex H: Proposed Operating Model & Temporary Access Protocol

A. Accredited User Access and WHOIS Providers

Upon accreditation, users are given credentials to access WHOIS data. Users can present their credentials to ICANN to include their IP address(es) in a whitelist. The whitelist should be operated by ICANN and administrated via the existing RADAR system. Contracted parties validate requesting IP address with the centralized list of whitelisted IP addresses, and are then able to deliver access to single record queries and automated access via port 43.

Access would be provided to approved parties under accreditation / certification mechanism or any applicable code of conduct.

At a high level:

1. Approved parties designate their rationale for access under GDPR, i.e. their legitimate reasons for accessing the data and the use(s) they will be put to.
2. Approved parties designate the IP addresses from which they wish to query WHOIS servers.
3. The accrediting bodies provide those IP addresses to ICANN, which collects the IP addresses and access (processing) rationale of each party into a single list.
4. All WHOIS server operators (registries and registrars) will be required to pick up that list from ICANN daily. They must whitelist WHOIS access from the approved IP addresses, and provide full WHOIS data ("thick" data, containing contact data) for queries coming from those IP addresses.
5. All port 43 operators must designate the locations of their WHOIS servers to be used for this authorized access program. A list of such will be maintained by ICANN and made available to the parties approved for access.

Security: Port 43 access managed by IP range is appropriately secure for this usage. IP address restrictions are a common and effective method to block access from public (non-approved) locations, and will allow only approved parties to gain access to the data. The approved parties should be required to provide IP addresses that will be used ONLY for WHOIS access, and not for any other purpose, so access is not possible from the entirety of their networks. Please note that IP address is one of the ways by which domain registry operators authenticate their accredited registrars for access to registry systems. While registries layer additional measures on top of IP-controlled access, that extra security is appropriate because registrars are gaining access to create and modify records and perform billable transactions. In contrast, WHOIS servers are separate from core registry systems (databases) and provide data only, no the ability to create or modify data.

B. Individual Queries

In addition to the web based lookups offered by registries and registrars, ICANN should continue offering WHOIS lookups for non-public data to those who have credentials. Both can use a simple, centralized, expedient and low-touch implementation tactic to provide access.

1. Leverage and extend the existing ICANN centralized WHOIS system (as hosted on the ICANN website here). Contracted parties provide ICANN with full, unlimited access to non-public WHOIS data via Port 43. Credentialed users submit individual queries from their whitelisted IP address(es) to the ICANN query mechanism and are granted access to individual non-public WHOIS records.
2. Leverage and extend existing web-based access provided by contracted parties. Contracted parties provide credentialed users the ability to submit individual queries from their whitelisted IP address(es) to their web-based form and grant access to individual non-public WHOIS records.

C. Temporary Access Protocol for Higher-Volume Queries

A similar Temporary Access Protocol should be developed and implemented for volume WHOIS queries until such time that RDAP is implemented across all contracted parties. Once RDAP is fully adopted, OpenID offers a current method for access -- please see Annex I for additional detail.

Annex I: Draft RDAP Open ID Connect Profile

This section defines a profile of the technical and operational requirements needed to support the identity, authentication and authorization mechanisms specified in draft-hollenbeck-regext-rdap-openid-07, describing a federated authentication system for RDAP based on OpenID Connect (OIDC)
Note: This section is a work in progress.

Trusted OpenID Providers (Ops)

The OpenID Connect framework allows for multiple (one or more) OPs to exist depending on the needs and requirements of the ecosystem. In a globally federated RDAP system one could imagine the existence of multiple OPs each providing identification and authorization services for their affiliated community of interest. (e.g. Law enforcement agencies, cybersecurity investigators, trademark and copyright investigators, certificate authorities, etc.). These communities may also be distinct per jurisdiction, as would be the case for law enforcement.

Alternatively, a single OP could support the needs of the whole community, issuing credentials to any entities able to prove that they have successfully met the requirements of an applicable RDAP Access Accreditation body.

In the case multiple OPs are used, each OP could be accredited and authorized by ICANN to issue and manage credentials to their user base. The OP accreditation process would leverage processes, infrastructure and resources currently used to accredit and de-accredit Registrars (and others) today. Once OPs are approved by ICANN, all RDAP server service providers would be required to support and trust credentials issued from the new OP, ensuring a consistent user experience across all RDAP servers.

Questions to be answered/discussed:

1. *Single vs. Multiple OPs.*
2. *ICANN as the single OP?*
3. *ICANN as one of many OPs?*
4. *OP Accreditation: Definition of Tech/Operational Requirements to become "trusted", Drafting of OPAA and OP Guidebook?*

Approved Authentication Mechanisms

Section 3.2 of RFC 7481 defines the requirements for clients and servers on the use of the authentication framework specified in "HTTP: Authentication" [RFC7235]. Either "basic" or "digest" authentication schemes can be used. Servers must support one scheme and clients must support both to ensure interoperability.

As support for TLS client/user authentication using X.509 certificates is OPTIONAL, this profile only requires the support of "basic" or "digest" authentication mechanisms. Certificate based authentication mechanisms may be considered in the future along with a suitable authorization technology.

Questions to be answered/discussed:

1. *Need to think about who or what we will be identifying. Individuals? Organizations? Systems that query WHOIS on behalf of users? All of the above?*
2. *For security purposes, should this profile mandate "digest" over "basic"?*

Query Purpose

As GDPR compliance requires an indication of the "purpose" of the RDAP query, this profile REQUIRES the use of the Stated Purpose claim as defined in Section 3.1.4.1 of draft-hollenback-regext-rdap-openid-07. The included

purpose claim will be used by the RDAP server to determine and authorize which data can/should be returned to the requestor. Clients and Servers conforming to this profile MUST support the following Query Purpose Values defined in section 6.3. –

- domainNameControl
- personalDataProtection
- technicalIssueResolution
- domainNameCertification
- individualInternetUse
- businessDomainNamePurchaseOrSale
- academicPublicInterestDNSRResearch
- legalActions
- regulatoryAndContractEnforcement
- criminalInvestigationAndDNSAbuseMitigation
- dnsTransparency

Questions to be answered/discussed:

1. *The above list is from the EWG report. Is there anything missing? Should any be removed?*
2. *Authorization token session length -- long or short? Can "purpose" be cached and used over time or must a new authorization be created and submitted for each query?*
3. *Can/should a single authorization request contain multiple Query Purposes?*

RDAP Response Profile

This section will define at least two RDAP response profiles i.e. what Registration Data fields will be returned based on successful authentication and authorization of the requestor.

Authentication/Authorization Level	**RDAP Response Profile**
None/None	Minimum Public Data Set Response Profile (Thin Data)
Valid/All	All Public and non-Public Data Set Response Profile (Thick Data)
Invalid/*	Minimum Public Data Set Response Profile (Thin Data)
Valid/Query Purpose 1	Query Purpose 1 Data Set Response Profile
Invalid/Query Purpose 1	Minimum Public Data Set Response Profile (Thin Data)
Valid/Query Purpose 2	Query Purpose 2 Data Set Response Profile
Etc…	

Once defined all compliant RDAP servers MUST adhere to the mapping above, ensuring a consistent user experience across all RDAP servers.

Questions to be answered/discussed:

1. *Are all Authentication credentials the same when it comes to data access? Or would LE be provided different access than others? If so, we would need to expand the above table.*

Annex J: Registration Directory Service Accreditation Authority High-Level Requirements

(Contributed by MarkMonitor and DigiCert)

Introduction

This document illustrates the high-level requirements for the Registration Directory Service Accreditation Authority (RDS AA) that issues X.509 public key certificates to those who seek access to the full domain registration data currently widely known as WHOIS. In a nutshell, the RDS AA issues credentials which could be used for Transport Layer Security[42] (TLS) client authentication in conjunction with the Registration Data Access Protocol (RDAP)[43][44][45][46][47] that is designed to replace the traditional WHOIS[48] protocol in the near future. Unlike the legacy port 43 WHOIS, which does not directly support any kind of authentication mechanism, implementing simple TLS client authentication to RDAP could be done with a relatively small effort as RDAP is HTTP based. In March 2018, the RDAP pilot working group started testing the usage of digital certificates for access control of RDAP. This technology is currently under extensive testing and evaluation and the results are expected to be published by end of July 2018.

There is currently an Internet draft regarding the usage of federated client authentication (password and ID) based on OpenID and OAuth. There may also be advantages to using digital certificates in conjunction with federated client authentication because each method allows a client to be identified and authenticated for different client-server interactions. A digital certificate can be used to identify and authenticate the client when establishing a secure connection to an RDAP server. Information encoded in the certificate can be used to determine if a client is authorized for access to an RDAP server. Digital certificates provide non-repudiation due to the nature of Public Key Infrastructure (PKI). Digital certificates can also be used to provide role-based access control (RBAC), making connection-approval decisions based on the attributes provided within the digital certificate. If the Internet community decides to adopt RBAC, there will be some application development work that would be required for RDAP. Federated client authentication based on OpenID and OAuth can be used to identify and authenticate a client for access to specific registration data elements because this service is performed directly within the RDAP application layer as part of processing an RDAP query. Fine-grained attributes, such as the purpose of an RDAP query, can be encoded in the client's identity and shared with the RDAP server software that needs to determine if a client is authorized for access to specific data elements. Both approaches leverage trusted third parties (Certificate Authorities for digital certificates and Identity Providers for OpenID/OAuth) that can be used to make the secure attestations of a client's identity and attributes that are needed to ensure that a client is authorized to receive the data they are requesting.

The RDS AA is expected to operate in a highly secure and transparent manner as essentially, it is a PKI service and the entity issuing the credentials is a Certificate Authority (CA). There are many items that would need to be taken

[42] RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2 https://www.ietf.org/rfc/rfc5246.txt
[43] RFC7480 HTTP Usage in the Registration Data Access Protocol (RDAP). A. Newton, B. Ellacott, N. Kong. March 2015. https://tools.ietf.org/rfc/rfc7480.txt
[44] RFC7481 Security Services for the Registration Data Access Protocol (RDAP). S. Hollenbeck, N. Kong. March 2015. https://tools.ietf.org/rfc/rfc7481.txt
[45] RFC7482 Registration Data Access Protocol (RDAP) Query Format. A. Newton, S. Hollenbeck. March 2015. https://tools.ietf.org/rfc/rfc7482.txt
[46] RFC7483 JSON Responses for the Registration Data Access Protocol (RDAP). A. Newton, S. Hollenbeck. March 2015. https://tools.ietf.org/rfc/rfc7483.txt
[47] RFC7484 Finding the Authoritative Registration Data (RDAP) Service. M. Blanchet. March 2015. https://tools.ietf.org/rfc/rfc7484.txt
[48] WHOIS Protocol Specification. L. Daigle. September 2004. https://www.ietf.org/rfc/rfc3912.txt

into consideration when running a CA however, this document will not attempt to be an exhaustive list of items that needs to be addressed but Instead, describe the high-level requirements for those to intend to run the RDS AA to facilitate the discussion in the Internet community.

RDS AA Framework Participants

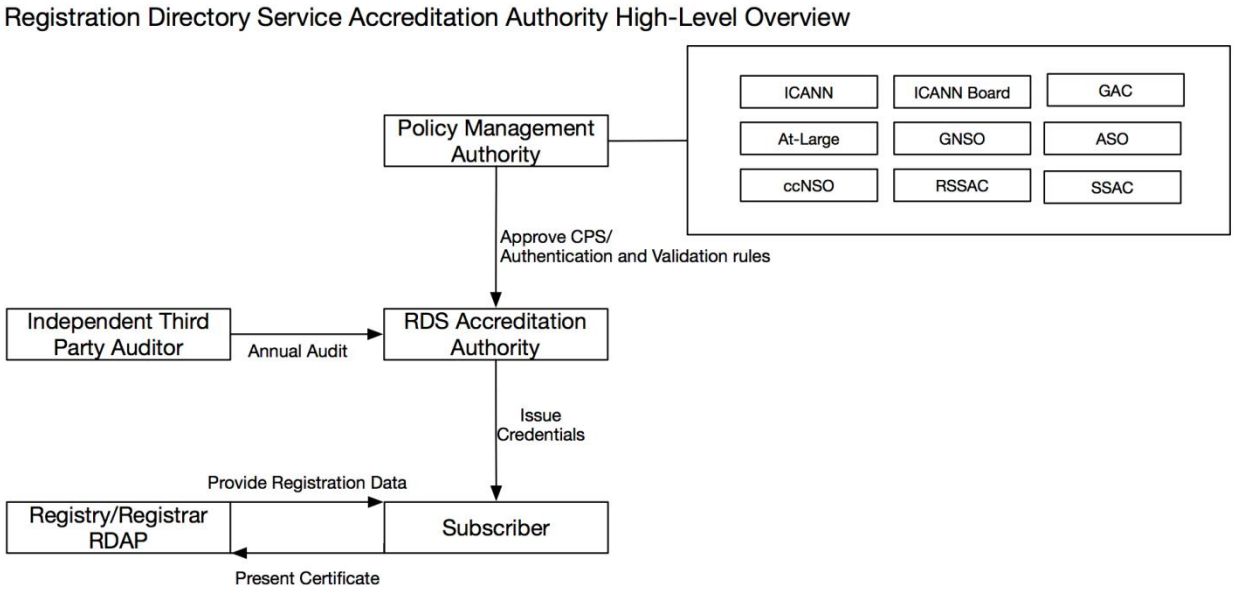

Figure 1

Figure 1 illustrates the participants in the RDS AA framework. The Policy Management Authority (PMA) is comprised of the representatives from each ICANN stakeholder groups and ICANN itself that will set the policies for the RDS AA. A Certificate Practices Statement (CPS)[49] will be submitted by the RDS Accreditation Authority for PMA review and approval. In case there is anything that is not clear to the RDS AA that would require interpretation of the Certificate Policy (CP) or the CPS, it will be escalated to the PMA. The PMA also sets the CP as a capstone document of this PKI service which each RDS AA will be required to adhere to in their CPS that describes the operational practices alongside with the security posture of the entity operating the CA. The PMA may choose the RDS AA based on the CPS and other information such as their track record, service levels, operational capabilities, security posture, third-party audit reports and so on. The PMA reviews and approves any update to the subsequent CPS at least annually. This framework allows efficient, secure and swift implementation of the policy to the accreditation process while assuring the due care and due diligence required to protect the RDS data. The amount of effort to establish such service will be hard for those who have no experience but would be relatively easy for those who have extensive experience in operating a CA. For further information on how a PMA is operated, refer to ISO/IEC 21188:2018[50]

[49] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, November 2003 https://www.ietf.org/rfc/rfc3647.txt
[50] ISO/IEC 21188:2018: Public key infrastructure for financial services -- Practices and policy framework International Organization for Standardization, Geneva, Switzerland.

The RDS AA will operate a CA issuing TLS client certificates used to access the full domain registration data on RDAP. The RDS AA is required to be audited annually by an independent[51] third-party auditor. The Subscribers are those who request access to the full registration information that resides on the RDAP server. After a successful authentication and validation, the Subscriber will receive a public key certificate corresponding to their private key. The Relying Party for the digital certificate are the Registries and Registrars who would operate the RDAP service as they will use the certificate as the basis for granting access. The trust anchor which is the root certificate and the intermediate certificate that issues the TLS client certificate will be configured on the RDAP server. Figure 2. is an example of the minimal CA hierarchy setup for the RDS AA. The CA hierarchy will be required to be at least a 3-tier hierarchy to accommodate online and offline key management. The cryptographic key for the root CA is managed offline and the cryptographic key for the intermediate/issuing CA would be online to issue the TLS client certificates. Depending on how the policy is set, the hierarchy is subject to changes. Figure 3. describes the TLS handshake when TLS client authentication is enabled between RDAP server and the RDAP client. It is worth noting that TLS client authentication does protect the service from man-in-the-middle attacks to simple TLS connections. For further information regarding TLS, refer to RFC524642. An RDAP pilot CA[52] was created as part of ICANN's RDAP Pilot Program[53] which adopts the hierarchy described below.

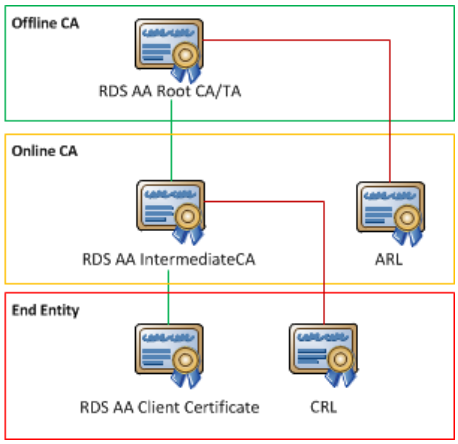

Figure 2

[51] AICPA Plain English Guide to Independence https://www.aicpa.org/interestareas/professionalethics/resources/tools/downloadabledocuments/plain%20english%20guide.pdf
[52] Digital Certificates for RDAP Pilot Client Authentication http://rdappilot.com/
[53] ICANN Community WIKI RDAP Pilot https://community.icann.org/display/RP/RDAP+Pilot

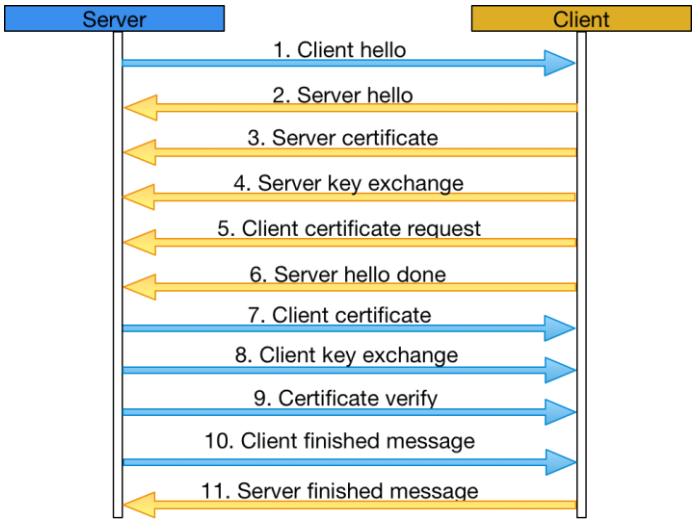

Figure 3

Qualification for the Registration Directory Service Accreditation Authority

- CA, Cryptographic Key and Token Lifecycle Management
  - Must be able to demonstrate proficiency in CA certificate management.
  - Must be well versed in cryptography to take precautionary actions to protect the Subscribers.
  - Must be capable of generating, storing, using and zeriozing cryptographic keys using hardware security modules.
  - Must have the infrastructure necessary to perform online and offline key management.
  - Capable of maintaining the ever-changing lifecycle of the cryptographic hardware security module such as end of sales/life, certification status change and product migration.
  - Must use HSMs that are certified at FIPS-140-2 Level 3 or above using trusted path authentication to protect the cryptographic keys of the CA certificates.

- Validation and Support
  - Must be able to provide 24/7/365 validation and support for the Subscribers.
  - Must be able to provide support in multiple languages in written and/or verbal form.
  - The 6 United Nation official languages which is the current standard for the ICANN community should be supported.
  - Must be able to handle global scale certificate enrollments in a reasonable amount of time. The RDS AA must have the capability to process at least 100,000 verification annum. at the level that is equivalent to the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (CABF BR)54.
  - The validation system must be flexible and scalable enough to handle large influx of validation requests.
- Third-party Audits
  - Must be able to undergo independent third-party audits that will qualify the RDS AA to operate as a CA.
  - The third-party audit must take place at least annually at the cost of the RDS AA.
  - Must be able to comply with the CABF BR.
- Revocation Mechanism
  - Must be able to authenticate a revocation request 24/7/365 and revoke the certificate in question immediately (TBD) once the request is authenticated.

- High Availability
    - All critical RDS AA information systems must be operated with a 99.9% or higher up time.

Qualification of the Independent Third-Party Auditor

As the only way to demonstrate an organization's accountability or to prove an organization's security posture in a publicly, transparent manner is to undergo third party audits, an independent third-party audit would be mandatory for the RDS AA. This will assure that the access credentials issued for the RDS complies with the criteria that is set by the Internet community. Fortunately, there is a well-established audit framework for CAs that allows the RDS AA to be highly scrutinized in order to establish trust among the Subscribers and the Relying Parties. CABF BR[54] outlines the qualification of the Third-Party Auditor for CAs as in Figure 4.

> *8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR*
> *The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:*
>
> 1. *Independence from the subject of the audit;*
> 2. *The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section8.1);*
> 3. *Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;*
> 4. *(For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO17065 applying the requirements specified in ETSI EN 319 403;*
> 5. *(For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;*
> 6. *Bound by law, government regulation, or professional code of ethics; and*
> 7. *Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors &*
>
> *Omissions insurance with policy limits of at least one million US dollars in coverage*

Figure 4

Validation and Authentication Process

An example of the enrollment information that could be vetted by the RDS AA includes, but not limited to the items listed in Figure 5. Depending on how the policy is set by the Internet community, the items that is vetted during the authentication and validation process are subject to change. Nevertheless, the RDS AA is at least expected to have the capability to perform authentication and validation for the items listed below which is laid out in the CABF BR in order to carry out the RDS AA responsibilities.

In addition to what is listed below, the RDS AA will be required to carry out other extra authentication and validation steps that would be specific to the RDS. An example is the authentication and validation items that are related to the General Data Protection Regulation (GDPR) that might include items such as, confirming the purpose/intent of the access to the RDS, compliance to the GDPR, acceptance of the subscriber agreement, pointer to their privacy policy, identifying the responsible party and contact information and so on. What is validated is

[54] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.6.pdf

subject to how the policy would be set for RDS by the ICANN community as a result of a dialogue with the EU Data Protection Authorities (DPAs).

3.2.2. Authentication of Organization and Domain Identity
If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this Section 3.2.2.1 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

3.2.2.1. Identity
If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. *A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;*
2. *A third party database that is periodically updated and considered a Reliable Data Source;*
3. *A site visit by the CA or a third party who is acting as an agent for the CA; or*
4. *An Attestation Letter.*

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address. Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.2. DBA/Tradename
If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. *Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;*
2. *A Reliable Data Source;*
3. *Communication with a government agency responsible for the management of such DBAs or tradenames;*
4. *An Attestation Letter accompanied by documentary support; or*
5. *A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.*

3.2.2.3. Verification of Country
If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section 3.2.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4. Validation of Domain Authorization or Control
This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact. Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names. The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.
The Random Value SHALL be unique in each email, fax, SMS, or postal mail. The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

3.2.2.4.3 Phone Contact with Domain Contact
Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.
Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

3.2.2.4.4 Constructed Email to Domain Contact
Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the atsign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value. Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed The Random Value SHALL be unique in each email.
The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

3.2.2.4.6 Agreed-Upon Change to Website
Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.wellknown/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. *The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or*
2. *The presence of the Request Token or Request Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.*

If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

3.2.2.4.7 DNS Change
Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character. If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

3.2.2.4.8 IP Address
Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

3.2.2.4.9 Test Certificate
Confirming the Applicant's control over the FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.

3.2.2.4.10. TLS Using a Random Number
Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

3.2.2.4.12 Validating Applicant as a Domain Contact
Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

3.2.2.5. Authentication for an IP Address
For each IP Address listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant has control over the IP Address by:

1. *Having the Applicant demonstrate practical control over the IP Address by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address;*
2. *Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);*
3. *Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.2.4; or*

4. *Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described.*

Figure 5

High-Level RDS Certificate Lifecycle

Figures 6 and 7 illustrate an example of certificate lifecycle management process for the RDS AA. The RDS AA is required to be able to manage and provide all infrastructure that supports the certificate lifecycle of the TLS client certificates. (MORE INFORMATION EXPLAINING THE CHART IS FORTHCOMING)

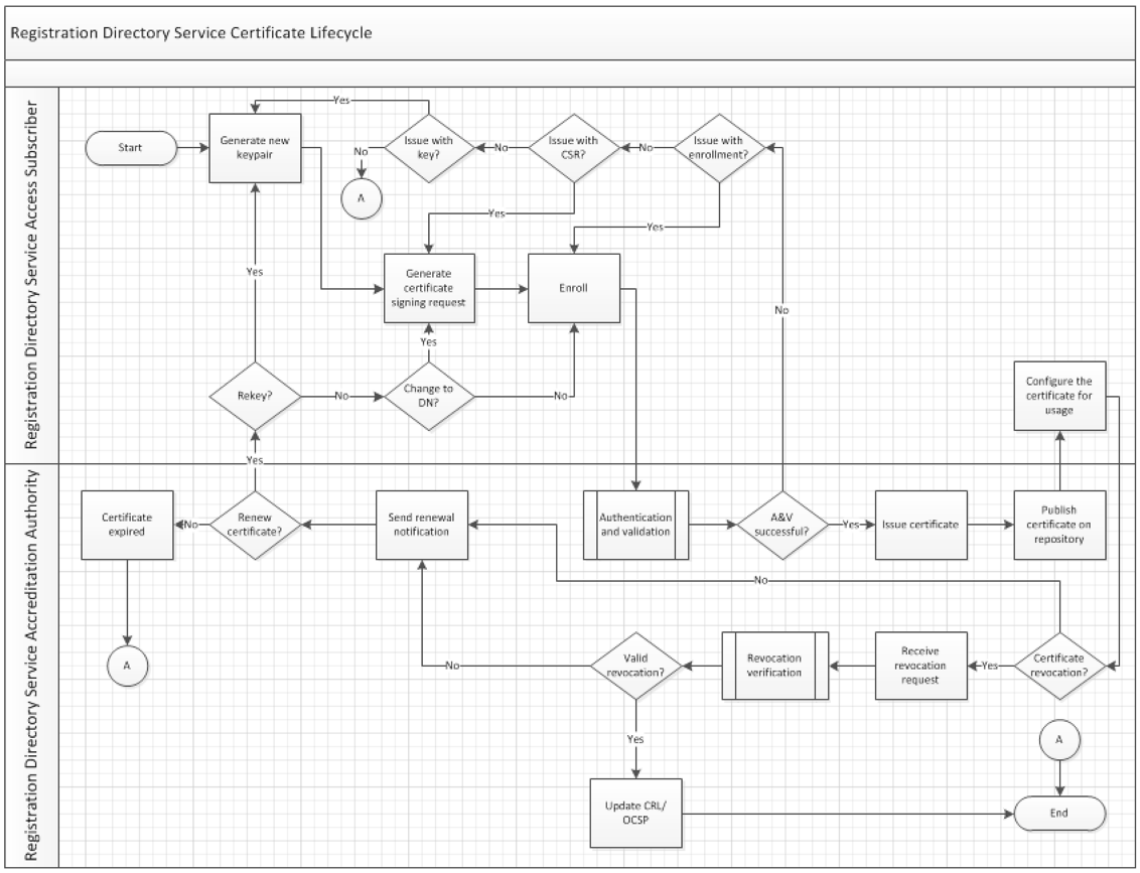

Figure 6

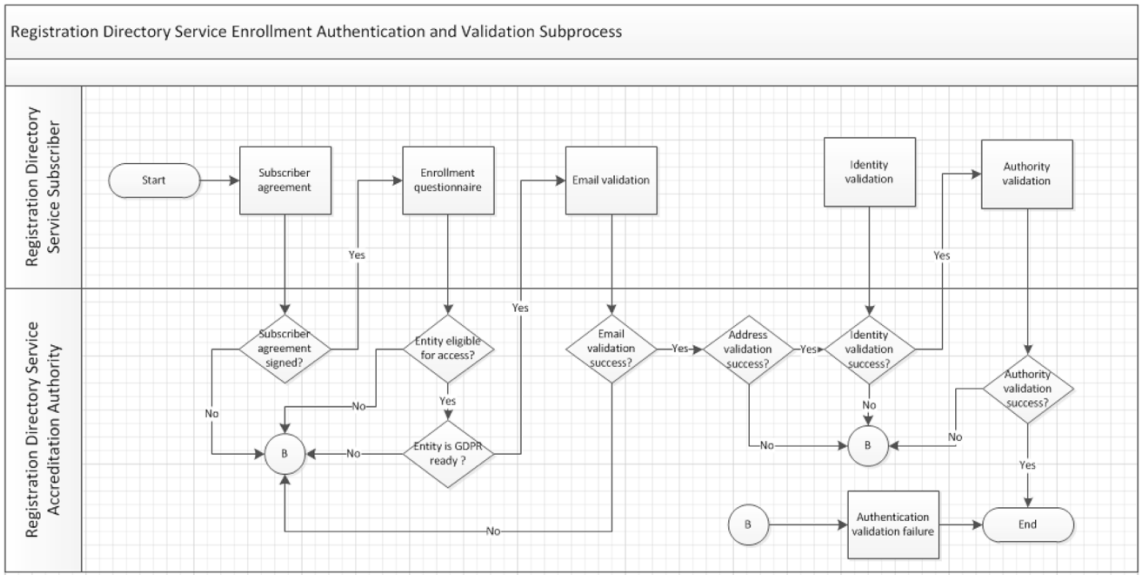

Figure 7

Overview of Security Management for CA Services

The RDS AA must establish their key management practices based on the best current practices. Figure 8. is an example of how risk-based security could be established for a CA. For those who go through an independent third-party audit are expected to have equivalent or similar practice when maintaining their security controls. The network and Certificate System Security Requirements[55] published by the CA/Browser Forum would provide some guidance on how the online systems should be protected. Aside from that, the RDS AA is required to demonstrate its capability in every aspect of Information Security and other operational practices through the CPS that is made public to the Internet community. (MORE INFORMATION REGARDING GENERAL SECURITY PROVISIONS WILL BE ADDED)

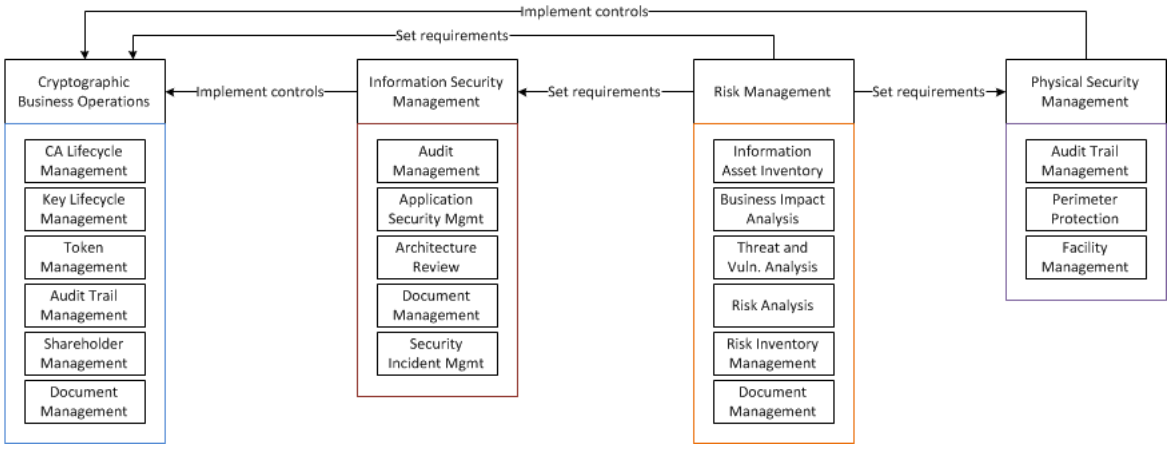

Figure 8

[55] CA/Browser Forum Network and Certificate System Security Requirements https://cabforum.org/wp-content/uploads/CABForum_Network_Security_Controls_v.1.1-corrected.pdf

Annex K: Lawful Bases for Access to WHOIS Data

Purpose for Processing	**Lawful Basis Under the GDPR**
Cybersecurity & OpSec Investigators	
Preventing fraud. Contacting victims of crime.	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party) *GDPR Recital 47: "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."*
Ensuring network and information security	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party) *GDPR Recital 49: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.* *This could, for example, include preventing unauthorised access to electronic communications*

	networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."
Cybercrime research; investigating trends related to safety threats	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party). *GDRP Recital 50: "Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations."* GDPR Recital 157: "In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law." See also: Recital 156.
Indicating possible criminal acts or threats to public security to a competent authority	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(d) (necessary in order to protect the vital interests of the data subject or of another natural person) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party). *GDPR Recital 50: "Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent*

	authority should be regarded as being in the legitimate interest pursued by the controller."
Initiating or facilitating legal proceedings	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party) *See also Article 9(2)(f)*
Determining accuracy of data, and reporting inaccurate data to the data controller(s)	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject). Article 5(1)(d) requires that "personal data shall be…accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');"
Intellectual Property Owners and Agents	
Investigating, tracking and preventing intellectual property infringement	Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Researching and investigating intellectual property infringement trends	Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Contacting infringing parties and relevant service providers	Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Identifying domains to support IP enforcement	Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)

Initiating or facilitating legal proceedings Maintaining intellectual property rights	Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Public Safety and Health Organizations	
Investigating, tracking and preventing activity that is dangerous to public health or safety	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(d) (necessary in order to protect the vital interests of the data subject or of another natural person) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Researching and investigating trends related to public health or safety threats	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Contacting victims of activity that is dangerous to public health or safety	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(d) (necessary in order to protect the vital interests of the data subject or of another natural person) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)

Identifying domains that may be involved in activity that threatens public health or safety	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(d) (necessary in order to protect the vital interests of the data subject or of another natural person) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Providing reports related to public health or safety threats to a government agency or law enforcement	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Initiating or facilitating legal proceedings	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(d) (necessary in order to protect the vital interests of the data subject or of another natural person) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Verification and Compliance by Private Parties, Companies and Service Providers	
Investigating fraudulent use of a domain name, of a registrant's name and/or other details in domain name registrations	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)

Investigating defamation, phishing, fraud, and other online abuse, and to determine the scope thereof	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Asset investigation and recovery in connection with civil disputes such as asset conversion, debts, and breaches of contract	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Locating a person for service of process in civil actions or other non-criminal legal procedures	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Identifying parties and non-parties in civil actions, proceedings, or potential actions or proceedings	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Identifying registrants in connection with the prosecution or defense of a civil action or other legal proceeding	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Performing contractual compliance and due diligence investigations	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject)

	Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Conducting registration data escrow audits and other regulatory and contractual audits	Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Validating website and domain name ownership and eligibility to conduct commercial activity	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Validating ownership in domain name purchase/sales transactions, brokering and escrow services	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Validating the transfer of domain names between registrars and/or registrants	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller)

	Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Investigating domain names, including historical records of domain names, registered to the same registrant in connection with purchases, sales, bankruptcy and receiverships, mergers and acquisitions, and other contractual and legal purposes	Article 6(1)(b) (necessary for the performance of a contract to which the data subject is party) Article 6(1)(c) (necessary for compliance with a legal obligation to which the controller is subject) Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)
Conducting journalistic, public interest and academic research	Article 6(1)(e) (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) Article 6(1)(f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party)