

**DRAFT WHOIS ACCREDITATION AND ACCESS MODEL
FOR NON-PUBLIC WHOIS DATA**

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

Table of Contents

I.	Overview	3
II.	Eligible Entities.....	4
	A. Cybersecurity and OpSec Investigators	4
	B. Intellectual Property Owners and Agents	4
	i. Accreditation Approach.....	5
	C. Public Safety and Health Organizations.....	5
	D. Verification and Compliance by Private Parties.....	6
	E. Accreditation Procedure	7
III.	Procedures.....	7
	A. Validation and Review of Access Purposes	7
	B. Process for Vetting and Accreditation	7
	C. Proposed Operating Model & Temporary Access Protocol	8
	i. Temporary access protocol.....	8
	ii. Permanent RDAP-based solutions.....	8
	a. RDAP Open ID Connect Profile	8
	b. Registration Directory Service Accreditation Authority (RDSAA)	8
	D. Logging	9
	E. Abuse Reporting	9
	F. Audit.....	9
	G. Fees and Renewal	9
	H. Complaints	9
	I. Penalties	10
IV.	Terms of Accreditation.....	10
	A. Data Protection	10
	B. Application Fees.....	10
	C. Data Access.....	10
	D. Data Forwarding.....	10
	E. Data Misuse	10
	F. Data Misuse Penalties.....	11

Annex A: Background

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

Annex C: Accreditation Approach for Cybersecurity & Opsec Investigators

Annex D: Accreditation Approach for Intellectual Property Owners and Agents

Annex E: Accreditation Approach for Public Safety and Health Organizations

Annex F: Verification and Compliance by Private Parties

Annex G: Proposed Operating Model & Temporary Access Protocol

Annex H: DRAFT RDAP Open ID Connect Profile

Annex I: Registration Directory Service Accreditation Authority (RDSAA)

I. Overview

This document provides a framework for the implementation of an accreditation and access model to provide access to non-public WHOIS data for legitimate and lawful purposes -- much like the “tiered access” model proposed in the Expert Working Group’s Final Report ([EWG Report](#)).¹

Building on ICANN Org’s proposed model that recognizes a legitimate basis for the continued collection of full thick WHOIS data by registrars, 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 **Annex B**), and (2) are properly validated by a third-party accreditor.

Documented here are:

- The types of eligible entities that may seek access to data;
- How eligible entities may be accredited to access data;
- A proposed operating model;
- Terms of accreditation; and
- Legitimate and lawful purposes for accessing data.

Note that this model does not include provisions for law enforcement agencies (LEAs) and other governmental access, which is extremely important and is being addressed by government representatives separately. 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.

¹ Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS) at p. 86

II. Eligible Entities: Purposes & Eligibility Requirements

The Eligible Entities highlighted here were initially derived from the list of entities and use cases documented in the EWG Report² and have evolved as a result of community feedback, but they are by no means an exhaustive list. The Eligible Entities listed here have legitimate and lawful purposes to access data, as well as agents that facilitate protection of public interests, security and lawful behavior.

A. Cybersecurity & OpSec Investigators³

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 purposes⁴ for access:

- 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 companies
- Security intelligence and analytics
- Ensuring continuity, integrity and availability of Internet infrastructures
- Domain risk scoring and blacklist / blocklist creation

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, JPCERT/CC, REN-ISAC, Akamai, BAE Systems, Cloudflare, IBM Security, Sophos, Symantec, DomainTools, Spamhaus and security organizations within companies like Salesforce, Facebook, Microsoft.

For more information, please see **Annex C**.

B. Intellectual Property Owners and Agents

² Id. at 21, See table of use cases in EWG report

³ SSAC members are working to create a proposal for appropriate credentialing of cybersecurity interests and are considering models like those used for the Anti-Phishing Working Group (APWG), their APWG Malicious Domain Suspension (AMDoS) model, and other relevant security vetting protocols. Other models that could be used include the Trusted Community Representative (TCR) used for DNSSEC.

⁴ A separate document correlating legitimate and lawful purposes to GDPR is forthcoming.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

This category is designed for intellectual property rights holders, (trademark, patent or copyright owners), or their agents (agents are legal representatives and brand 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. 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).

Legitimate and lawful purposes⁵ for access:

- 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

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
- Responding to trademark related claims
- Trademark clearance
- IP evaluation and investigation

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

Examples of entities in this category: Intellectual property attorneys, in-house corporate counsel, agents/staff of attorneys, and corporate-focused registrars (e.g. MarkMonitor and CSC).

For more information, please see **Annex D**.

i. Accreditation Approach

There are three generally recognized forms of intellectual property rights under generally accepted principles of international law: (a) trademarks, (b) copyrights, and (c) patents. We believe the existing Trademark Clearinghouse (TMCH)⁶ system can be used as the starting point for accrediting intellectual property owners in all three categories, in order to facilitate access to non-public WHOIS data for purposes of intellectual property investigations and enforcement. It would be helpful to establish a separate "Intellectual Property Accreditation Service System" (or "IPASS"), either as an individual department of the existing TMCH or as an affiliated or otherwise integrated entity, leveraging the existing TMCH validation staff and software systems to conduct accreditation of intellectual property owners in the three primary categories of intellectual property rights. Each of these categories of rights are discussed in turn in connection with possible accreditation criteria within **Annex C**.

C. Public Safety and Health Organizations⁷

⁵ A separate document correlating legitimate and lawful purposes to GDPR is forthcoming.

⁶ The Trademark Clearinghouse (TMCH) was established as part of the Rights Protection mechanisms (RPMs) adopted in connection with the 2012 new gTLD program. The new gTLD Registry Agreement (RA) incorporates the TMCH Requirements by reference in Section 2.8 and Specification 7. See ICANN, New gTLD Registry Agreement, Section 2.8, Specification 7 (July 31, 2017), available at <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html>; ICANN, TMCH Requirements (May 14, 2014), available at <http://newgtlds.icann.org/en/about/trademark-clearinghouse/rpm-requirements-14may14-en.pdf>.

⁷ 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 those organizations which have a mission of combating threats to public health and safety.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

Eligible Entities in this category are not-for-profit organizations that seek to protect public safety and health. 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 purposes⁸ for access:

- 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**.

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

This category is designed for private parties, companies and service providers that require access to WHOIS data in order to verify registration details and comply with legal obligations in the course of performing crucial tasks for private parties in the public interest.⁹ 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 on behalf of another person. Agents in this category are academics, legal professionals, accountants, journalists and others that need to conduct due diligence for themselves or on behalf of others.

Legitimate and lawful purposes¹⁰ for access:

- 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

⁸ A separate document correlating legitimate and lawful purposes to GDPR is forthcoming.

⁹ 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; See; <https://gdpr-info.eu/art-6-gdpr/>.

¹⁰ A separate document correlating legitimate and lawful purposes to GDPR is forthcoming.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

- 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, 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), Lazard, Morgan Stanley, Goldman Sachs, Barclays (M&A), Investigative Group International, Escrow.com, Payoneer, Carnegie Mellon University

E. Accreditation Procedure

The accreditation approach for this category encompasses three (3) types of “Accreditation Categories”:

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

Accreditation would be provided by an ICANN “Accreditation Review Panel” consisting of individuals who are expert in privacy policy, Internet functionality, as well as legal and business issues. The ICANN Accreditation and Review Panel would publish the criteria for access, which would encompass the three (3) Accreditation Categories, which are explained more fully in **Annex F** below.

III. Procedures

A. 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.¹¹ Appeal mechanisms will apply in the instance that a review results in de-accreditation.

B. Process for Vetting and Accreditation¹²

Users are to be vetted by the accreditation authority¹³ 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

¹¹ Much like the “Purpose-Driven Access” model proposed in the EWG Report, p. 10

¹² Note additional scenarios for accreditation - Id. at 63

¹³ 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 established by treaty and comprised of and accountable to its 191 member states.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

- 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
- 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.

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 -
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.

C. 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 by May 25, 2018 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 existing 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 G**.

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.¹⁴ Two examples of this are as follow.

a. RDAP Open ID Connect Profile

¹⁴ 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.

Annex H 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 I.

D. Logging¹⁵

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 service 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.¹⁶ 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.)."¹⁷

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.

E. 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 revoking accreditation.

F. 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 Principles18). Also, query logs should cite purposes of access, which must be tied to a legitimate and legal use for each accredited 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).

G. Fees and Renewal

Application and renewal fees should be sufficient to cover onboarding and support fees for the authorization and access

¹⁵ Logging responsibility decision 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 -- they would be responsible for logging.

¹⁶ [EWG Report](#), p. 91

¹⁷ [Id. at 116](#)

¹⁸ [Id. at 94](#)

system. Application and renewal fees should scale with the number of users for each accredited entity.

H. Complaints

- Complaints regarding accuracy of data will be addressed directly to the domain name's sponsoring registrar for resolution.
- Complaints regarding performance of underlying WHOIS providers will be directed to ICANN compliance, who will address the matter with the appropriate registrar, according to the terms of the Registrar Accreditation Agreement.
- All other available remedies (e.g., filing false WHOIS complaints) are available to all appropriate parties.
- Complaints regarding unauthorized access to, or improper use of, data will be relayed to the accrediting agency for appropriate remedial action (see following sections on Penalties and Data Misuse Penalties).

I. 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).

IV. 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 validation 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 code of conduct.

E. Data Misuse

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

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.¹⁹ 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 Principles²⁰) 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.

¹⁹ Further, depending on the nature of misuse, GDPR penalties may apply.

²⁰ [Id. at 62](#)

ANNEX A BACKGROUND

During the ICANN 61 meeting in San Juan, Puerto Rico, the community discussed an accreditation and access model to ensure continued Whois availability for eligible entities seeking data access. Based on feedback from many, including members of the contracted party house (registrars and registries) and security interests (e.g., some [SSAC](#) members), this model has been further refined. Several community-wide discussions of the model have since been held for additional input from the community. All members of the community were invited to these discussions and encouraged to submit additional written comments and input on the publicly archived and ICANN supported [The Accred-Model Archives](#) website. Comments received to-date are incorporated into this version (numbered 1.5) -- a descriptive document intended as the basis for creation of a functional specification for implementation. (For a similar approach, see the TMCH [Functional Spec Example](#))

Significant amounts of resources continue to be devoted to this proposed accreditation and access model through a broad-based effort to avoid the possibility that Whois effectively will “go dark” on May 25. (See **Annex A** for additional background on why this is critical to the safety and security of the Internet and its users).

We now seek further community input and formal ICANN Org support to execute upon this model, including resources for design and implementation on an accelerated timeline.

On May 25, 2018, the General Data Protection Regulation (GDPR) will come into effect. In advance of that date, the domain name community has been working together to stay as close as possible to the current WHOIS system and the current thick WHOIS policy -- while finding a solution that complies with GDPR.

As part of that compliance effort, ICANN Org has proposed a [model](#) for the WHOIS system that limits public access to WHOIS data and has made subsequent references to Board action on a temporary policy (or specification) to implement it before May 25, 2018. This model, without a mechanism for access to non-public WHOIS data for legal and legitimate purposes, would effectively disable a critical tool employed for the safe and stable operation of the DNS, the prevention of crime, conducting vital cybersecurity operations, the protection of consumers, the enforcement of intellectual property rights and other critical functions²¹. By ICANN's own [proposed timeline](#), access to WHOIS would not be implemented until December 2018 or later -- causing a prolonged WHOIS access outage.

This is a significant problem, considering:

- 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, phishing, botnet attacks, and distributed denial of service (DDOS) attacks to the grimmer, 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 proposed model will severely impair or prevent 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, will have their ability to comply with obligations impaired or prevented.
- Consumers will 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

²¹ 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.”

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

resulting in greater instances of fraud, theft and identity theft.

As a result, governments, law enforcement, businesses, intellectual property owners and Internet users worldwide have expressed concern. ICANN's [Governmental Advisory Committee \(GAC\)](#) has given consensus advice to the ICANN Board in its [ICANN 61 communique](#) to maintain WHOIS to the fullest extent possible and to mandate an access mechanism to non-public WHOIS data. 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. The ICANN Board and ICANN Org, however, have indicated that they will likely not comply with GAC advice. (cite reference)²²

²² <https://www.icann.org/en/system/files/correspondence/chalaby-to-ismail-05may18-en.pdf>

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 report²³ and ICANN’s Cookbook,²⁴ 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 domd 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, consistent with 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 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.

²³ [Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service \(RDS\)](#), p. 16

²⁴ The Cookbook, Section 7.2.1, at 34. <https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf>

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

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	<ul style="list-style-type: none"> -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

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>Business/Personal Domain Name Purchase or Sale</p>	<p>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.</p>	<p>Prerequisite for functioning marketplace for DNs</p>	<ul style="list-style-type: none"> -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 	<p>Registrants, potential DN buyers, resale agents, Registrars</p>
<p>Technical Issue Resolution</p>	<p>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 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.)</p>	<p>Providing security and stability of the DNS, consumer protection, and protection of Registrants expectation of service Providing a pathway for resolving technical problems/ issues</p>	<ul style="list-style-type: none"> - Validation of Registrant information -Provision of access to technical users. -Foregoing requires storage of access to technical contact information 	<p>Registries, Registrars (Network Operations); DNS service providers; cybersecurity experts</p>

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>Domain Name Certification</p>	<p>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.</p>	<p>Protecting registrant's interest in maintaining secure DN</p> <p>Providing consumer protection and security</p>	<p>Validation of registrant contact info for EV, DV, OV SSL certifications</p> <p>-Foregoing requires storage of and access to full WHOIS data</p>	<p>Certificate Authorities, SSL Certification providers, Registrants, Registrars</p>
----------------------------------	---	--	--	--

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>Individual Internet User Protection Security and Trust</p>	<p>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.</p>	<p>Safety, consumer trust and protection, validation of trustworthiness of the information provider.</p>	<p>-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</p>	<p>Consumers , online platforms, and the general public</p>
<p>Academic/ Public Interest DNS Research</p>	<p>Tasks within this purpose are academic public interest research 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.</p>	<p>Promotes broad range of research purposes to improve function, use security, and stability of the DNS; Supports freedom of expression and academic research</p>	<p>-Access to public data and certain non-public data in anonymized form. -Foregoing requires the storage, publication and access to WHOIS data</p>	<p>Students, research orgs, journalists, and academics</p>

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>Legal Actions</p>	<p>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.</p>	<p>Investigating and remediating possible IP infringement or other civil law violations</p> <p>-Preventing fraud and other forms of abuse</p> <p>-Facilitating the establishment, exercise, or defense of legal claims</p>	<p>-Disclose to third party IP rights owners; potential legal complainants</p> <p>- Facilitate identification of and 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 identity- validated data.</p> <p>-Foregoing requires the storage, retention, publication and access to the full WHOIS data; enabling reverse WHOIS lookup</p>	<p>IP lawyers; intellectual property owners, brand protection and enforcement services companies and associations; cybersecurity experts; Registrars; Registry Operators</p>
----------------------	---	--	---	--

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>Regulatory and Contractual Enforcement</p>	<p>Tasks within this purpose are tax authority investigation 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.</p>	<p>-Supports audit and enforcement of private and public legal obligations</p> <p>-Supports security, stability and trustworthiness of DNS</p>	<p>-Storing and disclosing data to regulators, ICANN and authorities entrusted with domain name dispute adjudication.</p> <p>-Foregoing requires storage, retention and access to WHOIS data.</p>	<p>Regulators, ICANN Compliance, Parties to contracts, Administrative and enforcement entities such as WIPO</p>
---	--	--	---	---

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>Public Health and Safety Protection and Criminal Investigation</p>	<p>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</p>	<p>Public health, safety and security</p> <p>Investigating cyber-crimes and cyber-enabled crimes;</p>	<p>-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</p> <p>-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</p> <p>-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 activity</p> <p>-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.</p>	<p>Law enforcement and government or private entities entrusted with enforcement responsibilities; public health and safety organizations, including victim advocacy organizations; digital crime/abuse teams.</p>
---	---	---	---	--

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>DNS Abuse Study, Investigation and Mitigation</p>	<p>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.</p> <p>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 necessary driving to attribution of these attacks to the individuals and organizations behind them.</p>	<p>Protecting Registrant from abuse and hijacking of Registrant's DN</p> <p>Consumer trust in the Internet</p> <p>Ensuring network and information security and stability of the DNS</p> <p>Combating unlawful or malicious/abusive actions negatively affecting secure and stable functioning of the DNS</p>	<p>-Providing access to Registrant data for the purposes of detecting and mitigating DNS abuse</p> <p>-Foregoing requires storage, retention, publication and access to WHOIS data; enabling reverse WHOIS lookup</p>	<p>Law enforcement and public safety agencies;</p> <p>Cybersecurity firms and individual cybersecurity analysts and experts;</p> <p>Online platforms</p> <p>Registry Operators, Registrars</p> <p>ICANN Compliance</p>
--	---	---	---	--

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

<p>ICANN DNS Oversight</p>	<p>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,</p>	<ul style="list-style-type: none"> -Promoting choice and competition and ensuring the stability, security, and resiliency of the DNS -Addressing contractual compliance obligations -Supporting audit and oversight functions 	<p>Storing and disclosing data to ICANN</p> <ul style="list-style-type: none"> -Foregoing requires storage, retention, publication and access to WHOIS data 	<p>ICANN organization</p>
----------------------------	--	--	--	---------------------------

Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5

ANNEX C
ACCREDITATION APPROACH FOR CYBERSECURITY & OPSEC INVESTIGATORS

[PLACEHOLDER: THE SECURITY COMMUNITY IS WORKING TO PROVIDE DETAILED CREDENTIALING CONTENT BASED ON OTHER SECURITY DATA SHARING PROTOCOLS IN USE BY THE CYBER SECURITY COMMUNITIES INCLUDING M3AAWG AND APWG]

**ANNEX D
ACCREDITATION APPROACH FOR INTELLECTUAL PROPERTY OWNERS AND AGENTS**

Accreditation Criteria

- a. Establishing Intellectual Property Rights
 - i. Trademark

ICANN already uses a system to validate trademark rights in connection with certain Rights Protection Mechanisms (RPMs) developed as part of the 2012 round of new gTLDs: the Trademark Clearinghouse (TMCH)²⁵. The TMCH is an independent mechanism through which third parties (Deloitte for front-end services, and IBM for back-end services) are contracted by ICANN to evaluate and record legitimate trademark rights as established through regional or national trademark registrations, statute or treaty, or court order.²⁶ Trademark holders or their designees (licensees or agents) may submit trademark records for recordal in the TMCH.²⁷ Section 2 of the TMCH Guidelines provide specific information that must be submitted in order for the TMCH to evaluate the validity of the pertinent trademark right, for each category of protected mark. For example, to record a mark based on a regional or national trademark registration (which is the most common method of recording trademarks in the TMCH), the trademark holder or agent must submit the following mandatory minimum information²⁸:

1. Name of mark
2. Registration number
3. Registration date
4. Jurisdiction
5. Description of goods and services class
6. Detailed description of goods and services
7. Status of the trademark holder (owner/assignee/licensee)
8. Organization
9. Full name
10. Address
11. Contact information (phone, fax (if any), and email address)

Alternatively, trademark owners who have previously obtained a court order attesting to the validity of the relevant trademark(s) could submit a copy of the relevant court order as proof of legitimate trademark rights, subject to the relevant submission requirements under TMCH Guidelines Section 5.4. Alternatively, trademark owners whose marks have been used in a successful UDRP or URS proceeding could submit a copy of the relevant UDRP or URS determination as proof of legitimate trademark rights; such submissions would be required to include the same information as is otherwise required for court-validated marks. Alternatively, if the relevant trademark rights are protected under statute or treaty, the trademark owner could submit a copy of the relevant statute or treaty as proof of legitimate trademark rights, subject to the relevant submission requirements under TMCH Guidelines Section 5.5.

In addition, the mark holder must also submit a signed declaration that the mark is in use and provide a supporting specimen of use.²⁹ Although in the existing TMCH system, this information is only mandated where the mark owner wishes to be eligible for Sunrise, we believe it should be required for accreditation to prevent gaming.

If the party seeking to record the mark is an assignee or licensee of the mark owner, they must submit an applicable assignee or licensee declaration.³⁰ Further, if the trademark registration database in the jurisdiction where the mark has been registered is not publicly available online, the mark holder must also submit a copy of the applicable registration certificate.³¹ In addition, if the

²⁵ See *id.* See also TMCH Guidelines, v.1.2 (Nov. 2013), available at http://trademark-clearinghouse.com/sites/default/files/files/downloads/TMCH%20guidelines%20v1.2_0.pdf.

²⁶ See TMCH Guidelines, Section 1.3: Scope.

²⁷ See *id.* Section 1.4.

²⁸ See *id.* Section 2.2.

²⁹ See *id.* Section 2.2.3.

³⁰ See *id.* Section 2.2.4.

³¹ See *id.*

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

registration would expire during the term of the TMCH record, the mark holder must also submit a copy of the trademark renewal paperwork.³²

For trademark holders who have already recorded marks in the TMCH, they could simply use their existing TMCH record and Signed Mark Data (SMD) file to fulfill the trademark rights validation criteria listed above. If the trademark holder is not already recorded in the TMCH, they could submit this information directly through IPASS solely for purposes of accreditation and not to record any rights in the TMCH itself.

Although the TMCH is currently under evaluation within the RPM Review PDP Working Group, we believe it has generally worked well in evaluating and recording valid and legitimate trademark rights on a global scale.

Accordingly, we would support use of the TMCH system as the basis for the proposed IPASS, including to serve as an accrediting body for trademark owners, their designees, and agents in connection with accessing non-public WHOIS data, subject to some additional criteria (discussed further below in Sections III(c)-(e)).

ii. Copyright

IPASS could perform a similar process to accredit copyright owners and their agents, using similar criteria as submitted in connection with trademark owner or agent accreditation.

Using the trademark recordal criteria in the TMCH Guidelines as a baseline, we propose that to demonstrate copyright rights that would serve as the basis of accreditation, the copyright holder or agent must submit the following mandatory minimum information:

1. Name of the copyrighted work
2. A description or other information reasonably sufficient to identify the copyrighted work
3. Date of creation of the copyrighted work
4. Registration number (if applicable)
5. Registration date (if applicable)
6. Jurisdiction
7. Status of the copyright holder (owner/assignee/licensee)
8. Organization
9. Full name
10. Address
11. Contact information (phone, fax (if any), and email address)

The copyright holder would also be required to submit a copy of the copyright work or works that are the basis of the accreditation request. If there are numerous works involved, submission of one relevant work should be sufficient. Alternatively, copyright owners who have previously obtained a court order attesting to the validity of the relevant copyright(s) could submit a copy of the relevant court order as proof of legitimate copyrights, in addition to remaining applicable information listed above. Other means of establishing the legitimacy of copyright ownership might include providing any applicable copyright notices or publication announcements, or other evidence establishing the existence of a valid copyright-protected original work of authorship.

If the party making the request is an assignee or licensee of the copyright owner, they must submit an applicable assignee or licensee declaration. Further, if the party making the request cites a registered copyrighted work, and the copyright registration database in the jurisdiction where the work has been registered is not publicly available online, the copyright holder must also submit a copy of the applicable registration certificate.

These requirements are all supported by the Berne Convention, an international copyright treaty with 175 signatories (including 175 UN member states, plus the Cook Islands, Holy See, and Niue).³³ The World Intellectual Property Organization is the official depository regarding the Berne Convention, and many of the requirements under the Berne Convention are also integrated into the World Trade Organization Agreement on the Trade-Related Aspects of Intellectual Property Rights (TRIPS), of which there are currently 164 members.³⁴

³² See *id.*

³³ See World Intellectual Property Organization (WIPO), Berne Convention for the Protection of Literary and Artistic Works (Sept. 28, 1979) and notifications of accession (last visited May 7, 2018), available at <http://www.wipo.int/treaties/en/ip/berne/>.

³⁴ See World Trade Organization (WTO), Agreement on the Trade-Related Aspects of Intellectual Property Rights (TRIPS) (Apr. 15,

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

These requests would also be subject to the additional criteria discussed in Sections III(b)-(d), below.

iii. Patent

Although patent owners are less frequent users of WHOIS data in connection with identifying and addressing patent infringement, there may be scenarios where such access is needed to perform patent enforcement work. Accordingly, IPASS could also be used to accredit patent owners and their agents, using similar criteria as submitted in connection with trademark owner or copyright owner or agent accreditation.

Using the trademark recordal criteria in the TMCH Guidelines as a baseline, we propose that to demonstrate patent rights that would serve as the basis of accreditation, the patent holder or agent must submit the following mandatory minimum information:

1. Name of patented invention
2. Registration number
3. Registration date
4. Jurisdiction
5. Description of patented invention (abstract)
6. Family ID
7. Application Number
8. Filing Date
9. Detailed description of patented invention (claims)
10. Status of the patent holder (owner/assignee/licensee)
11. Organization
12. Full name
13. Address
14. Contact information (phone, fax (if any), and email address)

If the party making the request is an assignee or licensee of the patent owner, they must submit an applicable assignee or licensee declaration. Further, if the party making the request cites a registered patent, and the patent registration database in the jurisdiction where the work has been registered is not publicly available online, the patent holder must also submit a copy of the applicable patent certificate. If there are numerous patents involved in connection with the accreditation request, submission of one relevant patent should be sufficient for purposes of accreditation.

These requests would also be subject to the additional criteria discussed in Sections III(b)-(d), below.

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,³⁵ 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 invention to be patented
2. Description of the relevant intended mark, work, or invention
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)

1994), available at https://www.wto.org/english/docs_e/legal_e/legal_e.htm#TRIPs.

³⁵ 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>.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

The requestor would need to submit documentation demonstrating efforts to identify or develop the proposed intellectual property right, and prior efforts to perform due diligence and clearance regarding same.

These requests would also be subject to the additional criteria discussed in Sections III(c)-(e), below.

c. User Verification

While the proposed IPASS criteria for trademark, copyright, and patent as described above would be sufficient for demonstrating the appropriate legal rights in connection with the legitimate purpose of accessing non-public WHOIS, the individual or organization actually being accredited will likely need to submit some additional proof of identity that confirms that they are actually who they say they are, and are authorized to act and are acting in connection with these legal rights.

We believe the proposed IPASS system would be able to accommodate this additional step, and propose the following additional information be required for submission to the proposed IPASS in connection with an accreditation request for intellectual property rights ("IPR") related purposes:

- i. If the IPR owner is an individual natural person:
 1. a copy of the individual's government issued identification (such as passport, driver's license, etc.), showing that the individual seeking accreditation is the same individual trademark/copyright/patent owner.³⁶
 2. Alternatively, if the individual is a member of a relevant intellectual property association or organization, they could submit a letter from this organization attesting that the individual is a member and that the organization has a reasonable basis for believing that the individual submitting the accreditation request is the legitimate owner of the relevant IPR.³⁷
 3. In addition, or alternatively, if the individual has been a complainant in a successful UDRP or URS proceeding, the individual could submit the relevant determination to establish proof of identity (this would only be relevant in the trademark context), with a note of verification from the dispute resolution provider.³⁸
 4. Alternatively, the individual could instead submit documentation demonstrating the creation of a "designated agent" under the United States Digital Millennium Copyright Act (DMCA) wherein the requestor is either the service provider or the designated agent (this would only be relevant in the copyright context), potentially with a note of verification from the copyright office (this would apply specifically to US entities, but there may be comparable systems in other jurisdictions).³⁹
- ii. If the IPR owner is a legal entity:
 1. A document demonstrating the establishment of the legal entity, such as a website screenshot, brochure, business license, tax certificate, Doing Business As documentation, Fictitious Name documentation, IRS 501(c)(3) determination letter, certificate of tax exemption, EIN/TIN verification letter, articles of incorporation, certificate of incorporation, articles of organization, or other

³⁶ Such proof of identity is often used in the domain name industry to verify an individual identity. See, e.g., GoDaddy, Change of Account/Email Update Form (last visited May 7, 2018), available at <https://www.godaddy.com/help/submitted-a-change-of-accountemail-update-form-4043>.

³⁷ Relevant organizations might include the International Trademark Association (INTA), European Communities Trade Mark Association (ECTA), International Intellectual Property Alliance (IIPA), or the International Association for the Protection of Intellectual Property. This function might also be something that could be performed by an international organization such as WIPO.

³⁸ UDRP and URS dispute resolution providers currently include WIPO, the Forum, the Arab Center for Domain Name Dispute Resolution, the Asian Domain Name Dispute Resolution Centre, the Czech Arbitration Court Arbitration Center for Internet Disputes, and MFSD. See ICANN, List of Approved Dispute Resolution Service Providers

³⁹ See U.S. Copyright Office, DMCA Designated Agent Directory (last visited May 7, 2018), available at <https://www.copyright.gov/dmca-directory/>.

2. evidence showing the legal establishment of the entity;⁴⁰
A copy of documentation establishing the right of the individual party submitting the accreditation request (such as an employee of the trademark/copyright/patent owner entity) to act on the entity's behalf, such as a letter of authorization specifically naming the representative(s) who should be accredited on the IPR owner's behalf.
 3. A copy of government issued identification of the individual acting on the IPR owner's behalf.⁴¹
 4. Alternatively, if the individual or the legal entity on whose behalf they are acting is a member of a relevant intellectual property association or organization, they could submit a letter from this organization attesting that the individual or entity is a member and that the organization has a reasonable basis for believing that the individual submitting the accreditation request is a legitimate representative of the entity that owns the relevant IPR⁴²
 5. In addition, or alternatively, if the entity has been a complainant in a successful UDRP or URS proceeding, the entity could submit the relevant determination to establish proof of identity (this would only be relevant in the trademark context), with a note of verification from the dispute resolution provider⁴³
 6. Alternatively, the individual could instead submit documentation demonstrating the creation of a "designated agent" under the United States Digital Millennium Copyright Act (DMCA) wherein the requestor is either the service provider or the designated agent (this would only be relevant in the copyright context), potentially with a note of verification from the copyright office (this would apply specifically to US entities, but there may be comparable systems in other jurisdictions).⁴⁴
- iii. If another authorized representative or agent of the IPR owner is making the request:
1. A letter of authorization copy of the engagement agreement or other similar documentary evidence of the legal representation or agency, and which specifically names the individual making the request on behalf of the representative entity or names all representative(s) who should be accredited on the IPR owner's behalf;
 2. A copy of the government issued identification of the individual acting on the IPR owner's behalf.
 3. Alternatively, if the individual or the legal entity on whose behalf they are acting is a member of a relevant intellectual property association or organization, they could submit a letter from this organization attesting that the individual or entity is a member and that the organization has a reasonable basis for believing that the individual submitting the accreditation request is a legitimate representative of the entity that owns the relevant IPR.
 4. In addition, if the agent is a licensed attorney, this individual could submit his/her license number and jurisdiction of licensure in order to receive fast-track or similar expedited accreditation service.
 5. In addition, or alternatively, if the authorized representative or agent has been a complainant representative in a successful UDRP or URS proceeding (this would only be relevant in the trademark context) or litigation involving the relevant IPR, the agent could submit the relevant determination or court order to establish proof of identity of the agent.

⁴⁰ Such proof of legal establishment is often used in the domain name industry to verify a legal entity identity. See, e.g., GoDaddy, Change of Account/Email Update Form (last visited May 7, 2018), available at <https://www.godaddy.com/help/submitted-a-change-of-accountemail-update-form-4043>.

⁴¹ See n. 14, *supra*.

⁴² See n. 15, *supra*.

⁴³ See n. 16, *supra*.

⁴⁴ See n. 17, *supra*.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

6. Alternatively, if the agent is named as attorney of record on an applicable trademark, copyright, or patent registration, the agent could submit the relevant documentation showing the attorney of record listing to establish proof of identity.
7. Alternatively, the individual could instead submit documentation demonstrating the creation of a “designated agent” under the United States Digital Millennium Copyright Act (DMCA) wherein the requestor is either the service provider or the designated agent (this would only be relevant in the copyright context).

d. Attestation

Accreditation requests would be accompanied by a good faith statement by notarized or accompanied by sworn statement, from the accreditation requestor that the request for accreditation is in connection with accessing data for a legitimate purpose, specifically IPR protection and enforcement, that the accredited party will not use the data for any other purpose, that the accredited party will comply with applicable data protection laws in handling any data it accesses as a result of being accredited, and that the accredited party will submit without prejudice to applicable jurisdictions for disputes arising from alleged improper disclosures caused by knowingly false statements made by the requestor, or from requestor’s or the IPR holder’s knowing misuse of non-public WHOIS information disclosed to it in connection with its accredited access to such data.⁴⁵

c. [Acknowledgement] (Alternative to “c” above)

Accreditation requests would be accompanied by an acknowledgment from the accreditation requestor that the request for accreditation is made in connection with accessing data for a legitimate purpose, specifically IPR protection and enforcement, that the accredited party will not use the data for any other purpose, that the accredited party will comply with applicable data protection laws in handling any data it accesses as a result of being accredited, and that the accredited party will submit without prejudice to applicable jurisdictions for disputes arising from alleged improper disclosures caused by knowingly false statements made by the requestor, or from requestor’s or the IPR holder’s knowing misuse of non-public WHOIS information disclosed to it in connection with its accredited access to such data.

⁴⁵ This language is adapted from ICANN, Draft Privacy & Proxy Service Accreditation Agreement (PPAA), Intellectual Property Disclosure Framework Specification (version Feb. 28, 2018).

Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5

ANNEX E

ACCREDITATION APPROACH FOR PUBLIC SAFETY AND HEALTH ORGANIZATIONS

[PLACEHOLDER WHILE WE WAIT FOR THIS COMMUNITY TO PROVIDE MORE INFORMATION ABOUT CREDENTIALING]

**ANNEX F
Verification and Compliance by Private Parties**

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 Review Committee 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 Review Committee 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 Review Panel which would evaluate each Specific Access Requests on a case-by-case basis, governed by specific criteria based upon identified legitimate purposes.

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

Because the recipient of Special Access Accreditation would have already been vetted by the Accreditation Review Panel, 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 Review Panel;

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

1. 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 Review Panel or the data is being provided to the client on whose behalf the services are being performed, as disclosed in the Accreditation application; and;
- All WHOIS data obtained through Accreditation will be subject to the data protection and security requirements specified by the Accreditation Review Panel; and
- Comply with all applicable laws and regulations, as well as any policies set forth by ICANN or the Accreditation Review Panel; and
- Indemnify against all claims and damages resulting from the Accredited person's failure to abide by the conditions of Accreditation.

2. 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/imposition of penalties and other remedies for inappropriate use/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.

3. De-Accreditation

De-Accreditation will occur when the Accreditation Review Panel determines that the Accredited person has materially breached the conditions of its Accreditation based upon either; a) a third-party complaint received; results of an audit or investigation by the Accreditation Review Panel; or 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, the posted bond may be forfeited in whole or in part, and other additional financial penalties may be assessed, including calling upon the indemnity provided by the Accredited person.

Accreditation Chart

Accreditation Category	Type of Access	Accreditation Provider
Regular Access	Ongoing access based upon initial approval of application for	ICANN Accreditation Review Panel

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

	Accreditation	
Special Access	Once Accredited, must submit and obtain approval for Specific Access Request on each occasion where access is required	ICANN Accreditation Review Panel 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 Review Panel

**ANNEX G
Proposed Operating Model & Temporary Access Protocol**

i. 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 the approved code of conduct or accreditation / certification mechanism.

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 white list 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 approve 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.

ii. 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.

iii. 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. On May 25, Port 43 will display the full non-public WHOIS record, but will be closed to public use and accessible only by whitelisted parties and ICANN. Credentialed users and systems can then access non- public WHOIS data via Port 43 using automated means. Again, once RDAP is fully adopted, OpenID offers a current method for access -- please see [Annex E](#) for additional detail.

ANNEX H 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. *Centralized ICANN run OP?*
3. *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-hollenbeck-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

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

- personalDataProtection
- technicalIssueResolution
- domainNameCertification
- individualInternetUse
- businessDomainNamePurchaseOrSale
- academicPublicInterestDNSRRResearch
- 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 I
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 Security⁴⁶ (TLS) client authentication in conjunction with the Registration Data Access Protocol (RDAP)^{47,48,49,50,51} that is designed to replace the traditional WHOIS⁵² 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 draft⁵³ regarding the usage of federated authentication (password and ID) however, there are several advantages to using digital certificates in conjunction with, or as an alternative method to federated authentication. First, the access to RDAP does not have to rely on the availability of the identity provider which is a third-party required for federated authentication to work. Second, the digital certificates provide non-repudiation due to the nature of Public Key Infrastructure (PKI). Third, digital certificates could provide flexible and scalable functionality. For instance, it could be used for enhanced access control such as role-based access control (RBAC) making 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. Fourth, identity providers are usually not under the tight scrutiny of an independent third-party auditor and are generally not used to processing a large amount of validation requests. Last but not least, when using digital certificates, the decision of whether or not to grant access is made entirely by the entity running the RDAP services instead of the identity provider which is a third party.

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 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.

⁴⁶ RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2 <https://www.ietf.org/rfc/rfc5246.txt>

⁴⁷ 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>

⁴⁸ RFC7481 Security Services for the Registration Data Access Protocol (RDAP). S. Hollenbeck, N. Kong. March 2015. <https://tools.ietf.org/rfc/rfc7481.txt>

⁴⁹ RFC7482 Registration Data Access Protocol (RDAP) Query Format. A. Newton, S. Hollenbeck. March 2015. <https://tools.ietf.org/rfc/rfc7482.txt>

⁵⁰ RFC7483 JSON Responses for the Registration Data Access Protocol (RDAP). A. Newton, S. Hollenbeck. March 2015. <https://tools.ietf.org/rfc/rfc7483.txt>

⁵¹ RFC7484 Finding the Authoritative Registration Data (RDAP) Service. M. Blanchet. March 2015. <https://tools.ietf.org/rfc/rfc7484.txt>

⁵² WHOIS Protocol Specification. L. Daigle. September 2004. <https://www.ietf.org/rfc/rfc3912.txt>

⁵³ Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect draft-hollenbeck-regext-rdap-openid-07 <https://tools.ietf.org/html/draft-hollenbeck-regext-rdap-openid-07>

RDS AA Framework Participants

Registration Directory Service Accreditation Authority High-Level Overview

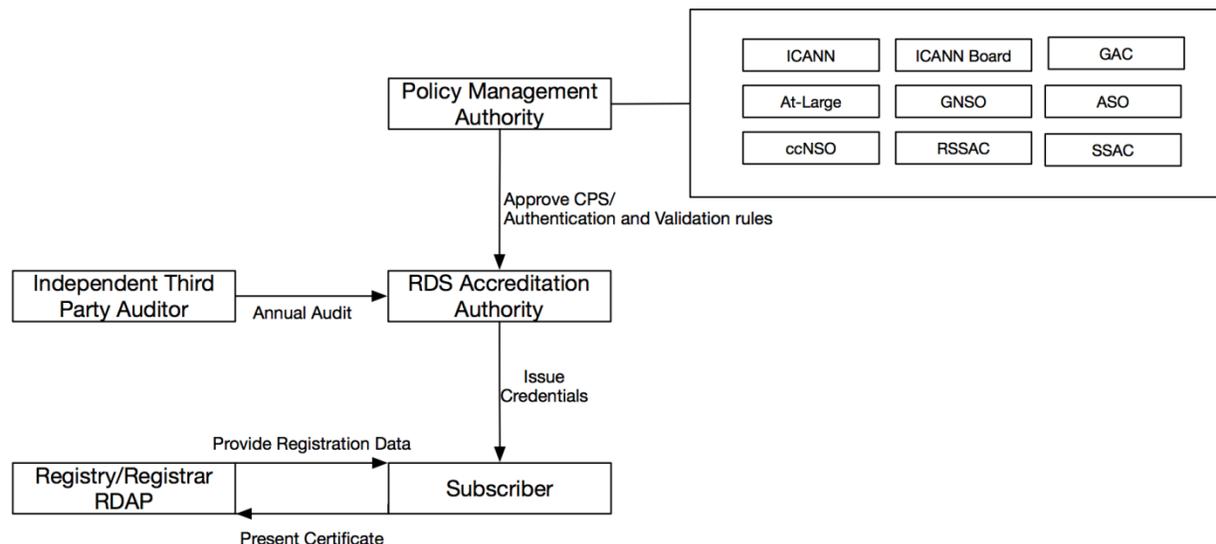


Figure 1.

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)⁵⁴ 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 21188:2018⁵⁵

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 independent⁵⁶ 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-

⁵⁴ 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>

⁵⁵ ISO/IEC 21188:2018: Public key infrastructure for financial services -- Practices and policy framework International Organization for Standardization, Geneva, Switzerland.

⁵⁶ AICPA Plain English Guide to Independence

<https://www.aicpa.org/interestareas/professionalethics/resources/tools/downloadabledocuments/plain%20english%20guide.pdf>

the-middle attacks to simple TLS connections. For further information regarding TLS, refer to RFC5246⁴⁶. An RDAP pilot CA⁵⁷ was created as part of ICANN's RDAP Pilot Program⁵⁸ which adopts the hierarchy described below.

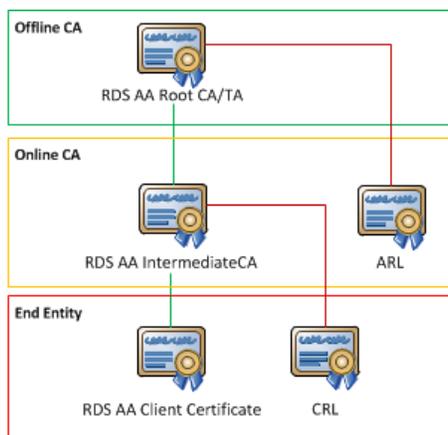


Figure 2.

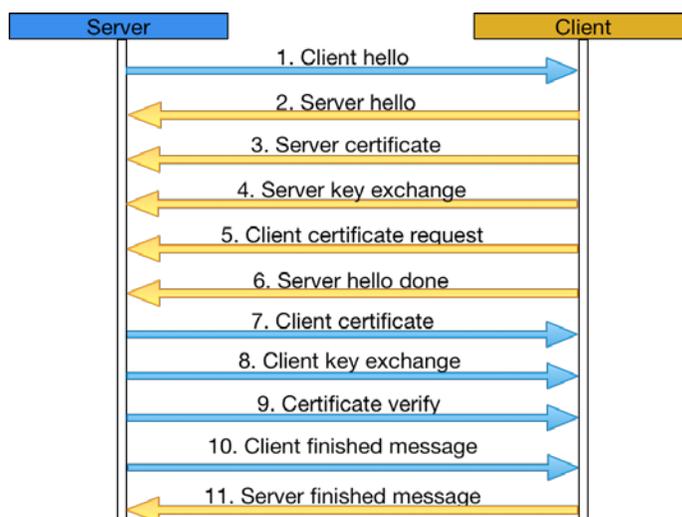


Figure 3.

Qualification for the Registration Directory Service Accreditation Authority

- o CA, Cryptographic Key and Token Lifecycle Management
 - o Must be able to demonstrate proficiency in CA certificate management.
 - o Must be well versed in cryptography to take precautionary actions to protect the Subscribers.
 - o Must be capable of generating, storing, using and zeroizing cryptographic keys using hardware security modules.
 - o Must have the infrastructure necessary to perform online and offline key management.
 - o 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.
 - o 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.

⁵⁷ Digital Certificates for RDAP Pilot Client Authentication <http://rdappilot.com/>

⁵⁸ ICANN Community WIKI RDAP Pilot <https://community.icann.org/display/RP/RDAP+Pilot>

- 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)⁵⁹.
 - 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 BR⁵⁹ 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 Section 8.1);*
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 ISO 17065 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

⁵⁹ 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>

**Draft Accreditation & Access Model
For Non-Public WHOIS Data
May 10, 2018
Version 1.5**

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 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

Figure 6 and 7. illustrates 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)

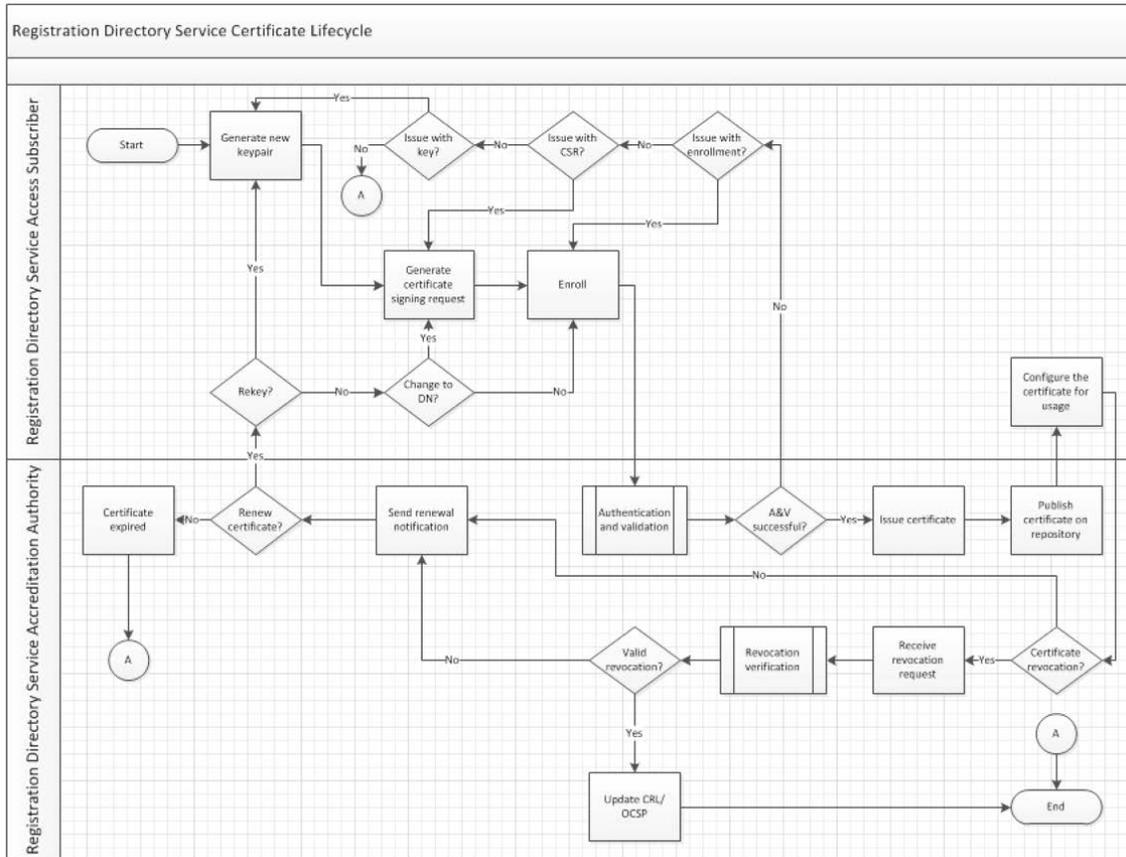


Figure 6.

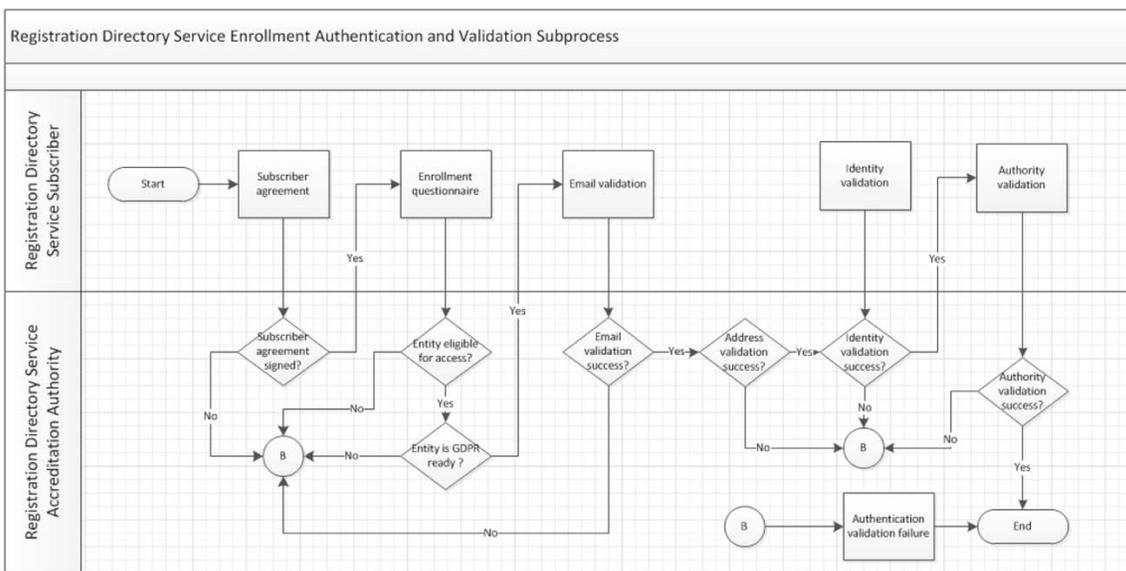


Figure 7.

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 Requirements⁶⁰ 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)

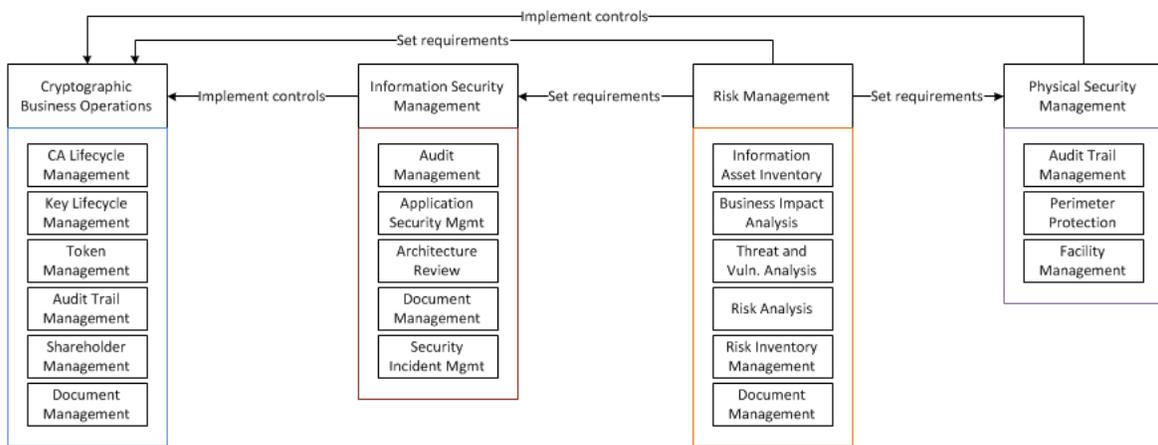


Figure 8.

⁶⁰ CA/Browser Forum Network and Certificate System Security Requirements https://cabforum.org/wp-content/uploads/CABForum_Network_Security_Controls_v.1.1-corrected.pdf