Draft Final Inventory of WHOIS Service Requirements

ICANN Meeting, Brussels, Belgium

Dave Piscitello, Senior Security Technologist

20 June 2010

BRUSSELS

ICANN

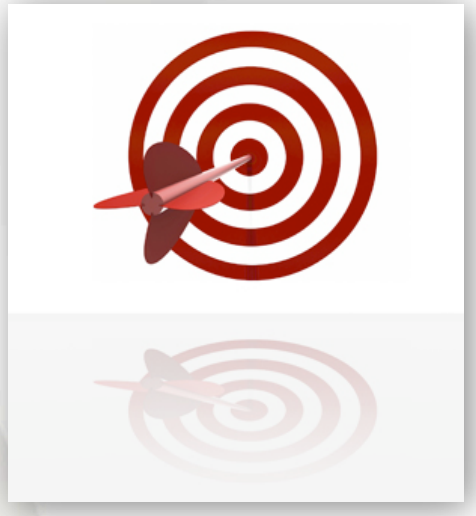
No.38 | 20-25 June 2010

Background

1. The GNSO Council requests that **Policy Staff**, with the assistance of technical staff and GNSO Council members as required, **collect and organize a comprehensive set of requirements for the WHOIS service policy tools**. These requirements should **reflect** not only the **known deficiencies** in the current service but should **include** any **possible requirements** that may be needed to support various policy initiatives that have been suggested in the past.

2. The synthesis of requirements should be done in consultation with the SSAC, ALAC, GAC, the ccNSO and the GNSO and a **strawman proposal should be prepared** for these consultations. The Staff is asked to come back with an estimate of when this would be possible.

Goals & Non-goals



Collect and organize a set of **technical requirements** for community consideration:

- Current features identified as needing improvement
- Features to support various, past policy proposals
- Features recommended by ICANN SOs, ACs, community

NOT gathering policy requirements

NOT recommending policy

Status of the report

- Released draft Report in March 2010, sent report to ALAC, SSAC, ASO, GNSO, CCNSO for input
- Conducted overview Webinars (April, May 2010)
- Received input from RySG (GNSO), ALAC, and a group of technical experts
- Incorporated comments and released Draft Final Report on May 31.

General Comments

- ALAC: The At-Large **supports all the requirements** expressed in the document, and believes there is a consensus in the community on these.

- RySG: “expresses appreciation for what we believe is very constructive report. We believe that it provides an **excellent basis for additional definition** of WHOIS service requirements for the future.”

Terminology

WHOIS service:

- WHOIS clients
  - Port 43 (text) clients
  - Web-based clients
  - Legitimate automation clients
- WHOIS servers
- Registration data

Terminology - comments

ALAC

- disagrees that web-based be considered "WHOIS clients" because they do not suffer from the same limitations as the text-based clients, and can easily handle authentication, internationalization and anti-abuse features

Preliminary Compilation:

- Mechanism to find authoritative Whois servers
- Structured queries
- Standardized set of query capabilities
- Well-defined schema for replies
- Standardized errors
- Quality of domain registration data
- Internationalization
- Security
- Thick vs. Thin WHOIS
- Registrar abuse point of contact

Mechanism to find authoritative WHOIS servers

- A list of domain names and IP addresses of authoritative WHOIS servers will serve users better than
  - Clients heuristics,
  - Preconfigured tables
  - (a priori knowledge)

Mechanism to find authoritative WHOIS servers

R1: Provide a publicly accessible and machine parseable list of domain names or IP locations of WHOIS servers

Structured queries

Server applications vary with respect to format of query data

e.g. To query AS number

ARIN: whois -h whois.arin.net a 6

RIPE: whois -h whois.ripe.net -Taut-num as7

e.g. To control IDN responses:

.DK: --charset=latin-1

.JP : /e

.DE: -c UTF-8

Structured queries

R2: Define a standard query structure that clients can implement and that all gTLD registries and ICANN accredited registrars will support

Standardized Set of query capabilities

- Past GNSO and SSAC reports have called for expanded query capacities beyond domain names
- Some registries offer expanded search capabilities today

Standardized Set of query capabilities

R5: Permit users to submit (any) registration data element as a query argument

Standardized Set of query capabilities - comments

RySG:

- Such searches do pose **significant technical issues**, and indeed it might not be possible to deliver such searches under contractual Service Level Agreements (SLAs).
- May facilitate **malicious activities**.

ALAC, Technical experts:

- **Privacy Concerns**

Structured responses

- No standardized format exists for data that registrars and registries return in responses to WHOIS queries

Structured responses

R3: Define a standard data structure for WHOIS responses

R3: The data structure should provide for correct identification, syntax and semantics of each data element

Structured responses - comments

ALAC:

"The use of a structured data model would **allow for easier localization of the client software**. This would be most welcome by those who do not have English as one of their languages and do not understand what "tech-c" may mean."

Standardized errors

No standard set of error messages is defined for WHOIS servers

WHOIS servers handle errors differently

Lack of standard error messages creates ambiguity and confusion

Standardized errors

R4: Define a set of standardized error messages and standard handling of error conditions

Examples of errors that could be standardized:

- Number of queries exceeds the limit
- no records found
- unable to process query

Quality of domain registration data

Are the data accurate?

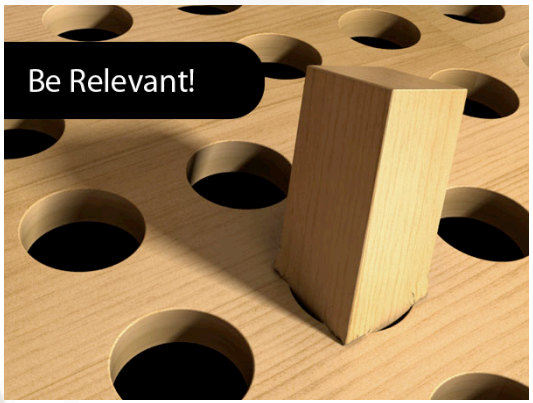
Are the data useful or relevant?

Are the collected data current?

Barriers to WHOIS accuracy

- Privacy Considerations
- Stealth, intentional deception
- Little or no corroboration of submitted data
- User error

Relevance (Utility) of WHOIS data



- Certain registration data are not as useful today as they were 20 years ago
- A future Whois data model should accommodate extensibility and changeability

Quality of domain registration data

R6: Adopt a structured data model for WHOIS data that provides extensibility and changeability properties

R6b: Add a time stamp to WHOIS data to show when the field was last verified or updated

Quality of domain registration data – ALAC comments

"The introduction of a **structured data format** would also be an excellent opportunity to require the **use of internationally agreed standards** on the display of postal addresses and phone numbers.

The use of a **machine-parsable output** would certainly be beneficial for legitimate uses of the WHOIS information. it will also make the life of those with malicious intents much easier, too.

There should be mechanisms put in place to **prevent large scale harvesting of data** for malicious use."

Internationalization

- No standard exists today for handling the submission and display of registration data from local languages and scripts
- Some Whois applications or services can only process registration data that are USASCII-7
- Deferring to the IRD-WG on their recommendations

Security

- Current WHOIS services do not support identity assertion, credentialing (verification), or data authentication

Need for Security

- Provide mechanisms to distinguish natural persons from artificial persons
- Protect (Discourage harvesting and mining of) personal identifying information

Security Frameworks

- Authentication
- Access Control
- Auditing

WHOIS security frameworks

- Authentication framework:
  - **Anonymous access and verification of identities** and a choice of authentication methods and credentials
- Authorization framework
  - Granular **access controls** (per registration data object permissions)
- Auditing framework
  - **Metrics** to accommodate future policy development for auditing WHOIS access

Security - comments

ALAC:

- "The authentication framework, coupled with granular access to data for the WHOIS service should not be an option or a nice to have feature, but is **a fundamental prerequisite to allow for the protection of the privacy of individuals.** It should be sufficiently flexible to allow those outside the gTLD community, notably ccTLDs, to implement access policies required by their local laws."

Registrar abuse point of contact

- Registrars and registries should provide and publish abuse point of contact information as an element of a domain registration record

Additional Requirements - RySG

- Ensure consistency of data between registries and registrars (for thin registries).
- Accommodate privacy services in a manner that effectively provides access to information
- Mitigate impacts to SLAs and EPP (Extensible Provisioning Protocol) commands in migrations from thin to thick WHOIS data.

Suggested Next Steps - RYSG

- "As the community moves forward with regard to new WHOIS requirements an important question for inclusion in the Initial Report is **which of the proposed requirements in this section involve Internet standards issues** that are the responsibility of the Internet Engineering Task Force (IETF). … we recommend that any standards work that may be needed be identified and steps taken to initiate the any needed standards development work as soon as possible so as to avoid possible delays later when additional WHOIS policy work may occur."

Suggested Next Steps – ALAC, Experts

- "we recommend the community **discuss** what services / protocols would satisfy these requirements and how **to move forward** to make these changes." (Technical experts)
- "The At-Large would like to see a clear **roadmap** and a **timeline with milestones** for the implementation of the above requirements."
- Whatever new solution is chosen / changes are made, we need some sort of **backwards compatibility** / phased introduction / transition plan. (Technical experts)

Thank you

BRUSSELS

ICANN

No.38 | 20-25 June 2010

Questions