VERISIGN®

WHITE PAPER

REGISTRATION DATA ACCESS PROTOCOL (RDAP) IMPLEMENTATION EXPERIMENTS AT VERISIGN

VERISIGN LABS LAUNCHED AN EXPERIMENTAL IMPLEMENTATION OF THE REGISTRATION DATA ACCESS PROTOCOL (RDAP) IN JANUARY 2016. THE PURPOSE OF THE EXPERIMENT IS TO DEMONSTRATE THE NEW CAPABILITIES BUILT INTO RDAP THAT ADDRESS THE MANY DOCUMENTED DEFICIENCIES OF WHOIS.

This implementation was designed based on these architectural principles:

1. Keeping data with its authoritative (original producer or collector) source to avoid unnecessary transfer of data thus reducing the risk of disclosure and allowing operators to respond to queries using data that they originally produce or collect.
2. Leveraging a distributed delegation model to respond to Registration Data Directory Services (RDDS) queries.
3. Leveraging standards-based client authentication, authorization and access control to protect personally identifiable information (PII, such as names, addresses, telephone numbers, etc.) from unauthorized access or unintended disclosure, and to ease implementation and adoption.
4. Having the authoritative sources provide standards-based RDDS interfaces to satisfy the needs of clients in a scalable and secure manner.
5. Leveraging standards-based clients to make it more efficient for RDDS users to query across registries, registrars and RDDS services.

PURPOSE

RDAP provides an opportunity for the domain name ecosystem to enable RDDS services without the need to replicate data and address local data privacy requirements, which may include laws or regulations. This model has been implemented as an RDAP service that leverages public interfaces to transparently receive user queries and provide complete responses. This service is described in this paper as the "Virtual Thick RDAP" (VTRDAP) service. A web interface can be found at https://vtrdap.verisignlabs.com/.

IMPLEMENTATION DETAILS

Figure 1 depicts the interaction between various RDAP services that work together to provide a complete query response to a user. The components are:

- **RDAP User**: The user that wants information from the RDAP services. The RDAP user uses an RDAP Client to resolve a query.
- **RDAP Client**: An application that interfaces with RDAP services and the RDAP Authentication Provider to resolve a query for an RDAP user. Many kinds of RDAP Clients can be created, including web clients

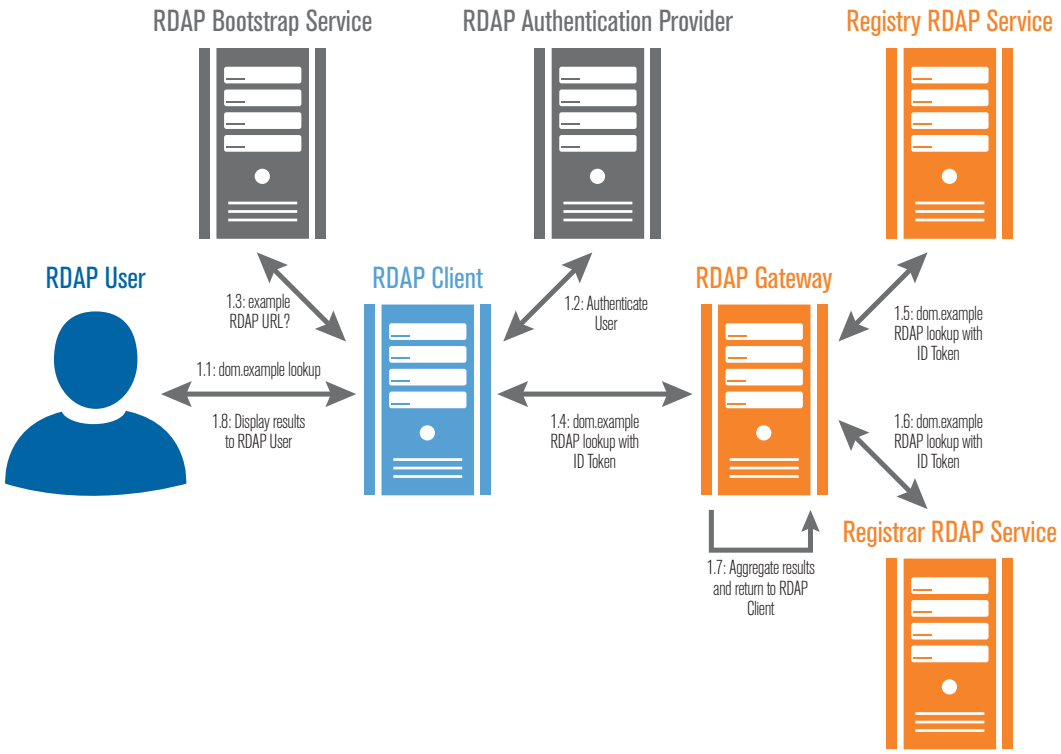
and command line clients. RDAP Clients could be leveraged to aggregate results across multiple registry and registrar RDAP services.

- **RDAP Bootstrap Service**: The HTTP service defined in RFC 7484 that provides the authoritative list of registry RDAP Service URLs for top-level domains (TLDs). The service returns a JavaScript Object Notation (JSON) response and is accessed using the URL, http://data.iana.org/rdap/dns.json. There is a single RDAP Bootstrap Service.
- **RDAP Authentication Provider**: A Federated Authentication Provider that supports RDAP user authentication, based on draft-hollenbeck-regext-rdap-openid, a draft protocol specification that is being considered for publication as an Internet RFC. The provider generates ID tokens that can be passed to the RDAP services to perform authorization. There can be more than one RDAP Authentication Provider. This can be leveraged for TLD operators that are contemplating needs for tiered authentication. It also provides flexibility for new security services should future policy define this as a requirement.
- **Registry RDAP Service**: RDAP Service provided by the registry that returns data that the registry produces or collects, such as the name servers associated with the domain. There would typically be one Registry RDAP Service per TLD.
- **Registrar RDAP Service**: RDAP service provided by the registrar that returns data that the registrar is authoritative for, such as registrant contact information. There would be at least one Registrar RDAP Service per registrar.
- **RDAP Gateway**: A service interface that acts as a "thick" registry interface from the RDAP Client's perspective. The gateway receives an RDAP query and assembles a complete, "virtual thick" RDAP response to an RDAP query. It does so by aggregating the responses to queries sent to the Registry RDAP Service and the Registrar RDAP Service.

MEASUREMENTS

To show the utility of VTRDAP, two types of measurements are presented, each focusing on a different benefit provided by the virtual thick model. First, the benefits of a distributed RDAP Service are shown via when each component from Figure 1 receives an RDAP query. This conveys how the virtual thick approach targets RDAP requests at the authoritative sources for the queried information, while avoiding queries to non-authoritative sources.

FIGURE 1: GENERIC TLD REGISTRY VTRDAP COMPONENT DIAGRAM



Second, it shows how authorization levels enable each downstream RDAP implementation to customize the amount of information returned by making access control decisions based on client identity and authorization. This highlights the flexibility of the virtual thick model to not only send queries to specific RDAP endpoints, but to let those specific RDAP endpoints make decisions about the information to reveal based on their applicable policies. For example, the registrar RDAP service policies may differ from the registry RDAP service. The query types measured included all possible query type combinations visible in the VTRDAP user interface, along with larger sets of 100 valid, auto-generated VTRDAP queries for each search type. These queries are then used to report on the average size of the information revealed. The measurements indicate that clients with higher levels of authorization will receive significantly more information than an unauthorized client.

RESULTS

Virtual Thick RDAP only sends requests for information to the authoritative source, as illustrated in Figure 2. Only domain queries hit both the registry and registrar RDAP services, as domain RDAP responses include authoritative information from both the registry (domain and name server) and registrar (entity). This contrasts with name server queries that only target the registry RDAP service and entity queries that only target the registrar RDAP service, which highlights the ability of VTRDAP to direct queries to authoritative sources. The targeting of requests to authoritative sources also leads to less duplication of information across registries and registrars.

IMPACT OF AUTHORIZATION

The authorization level provided by VTRDAP has a meaningful impact on how much information is returned for each RDAP request. To show this difference, Figure 3 displays the results from 100 randomly selected RDAP search queries for five different search types and shows the average resulting response sizes.

For domain name queries, the graph reveals how PII access can be controlled by authentication levels at the registrar. Responses to unauthenticated queries have the smallest size as they only contain domain information needed for resolution. Larger responses containing limited registrar-provided personal information occur for the Gmail Identity provider. The largest responses occur for the Verisign Labs implementation which provides the highest level of authorization and returns all available personal information.

For name server queries, the virtual thick implementation treats unauthenticated and Gmail identity provider access identically, returning the publicly available name server and IP addresses associated with that name server. Users authenticated with the Verisign Labs identity provider gain access to Extensible Provisioning Protocol (EPP) server-based status codes stored in the registry RDAP endpoint, resulting in the larger RDAP response sizes observed.

FIGURE 2: ENDPOINTS HIT FOR EACH RDAP QUERY TYPE

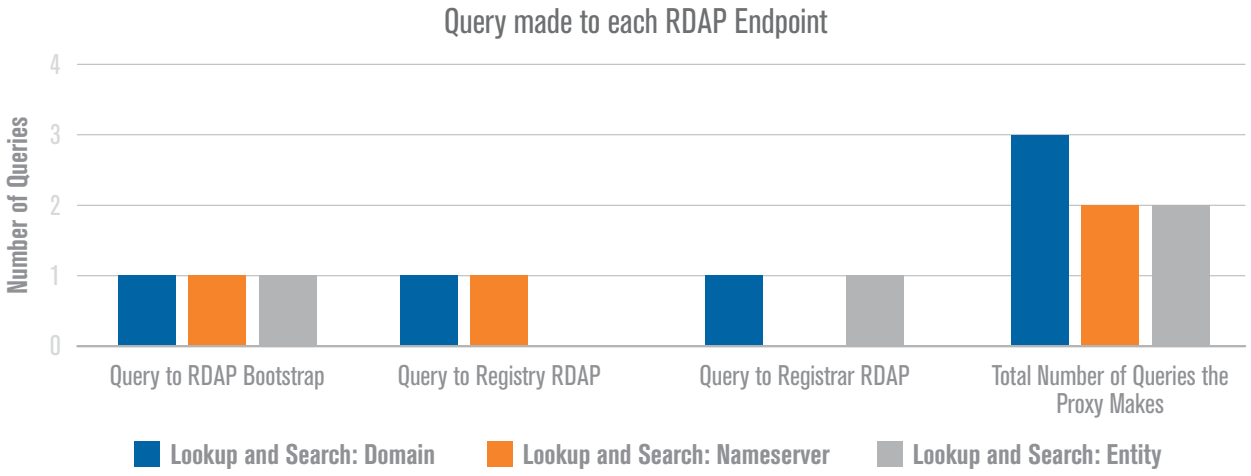
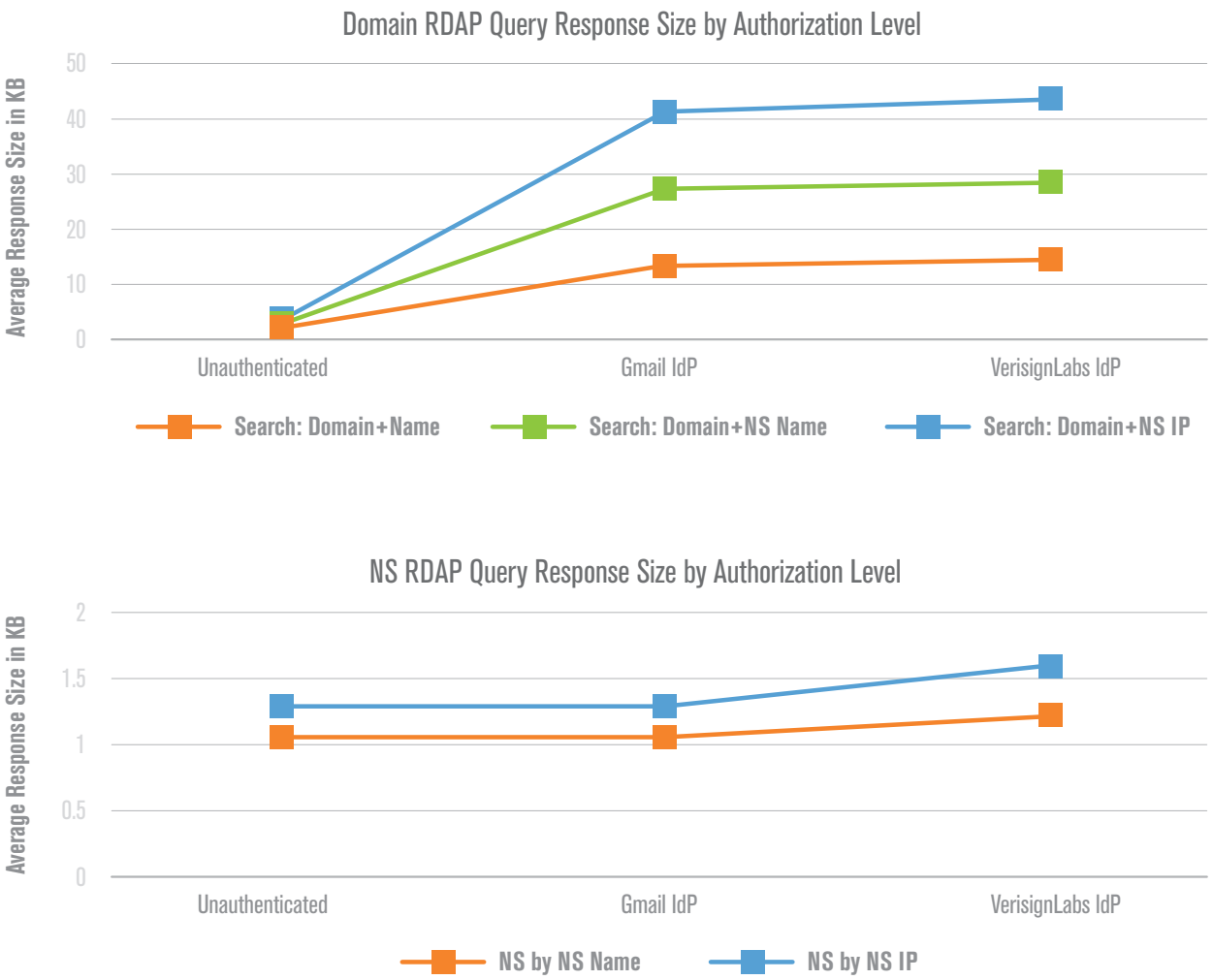


FIGURE 3: RDAP QUERY RESPONSE SIZES



CONCLUSION

The VTRDAP architecture serves as a sample implementation of the RDAP protocol that improves the quality and provenance of domain registration data while protecting personal privacy. This reduces the unnecessary transfer of PII and eliminates costly and difficult integration points between entities.

FUTURE PLANS

Verisign currently supports queries for domain names, name servers and entities in the .cc and .tv country-code TLDs. We hope to expand the service to gTLDs in the future. We will continue to update the model based on evolving protocol proposals and policy discussions. Please visit https://vtrdap.verisignlabs.com/ to participate in our ongoing experiments.