
ICANN
ANNUAL GENERAL
63
BARCELONA
20–25 October 2018

# Understanding RDAP and the Role it can Play in RDDS Policy

ICANN 63
22 October 2018

# Agenda

- Introduction
- RDAP Implementation Status in gTLDs
- RDAP: Mechanism and Policy
- Authentication and RDAP
- Registrar Perspectives on RDAP
- RDAP Client Demo

# Introduction

# Issues with (port-43) WHOIS

- No standardized format
- Lack of Support for Internationalization
- Unable to authenticate and thus provide different outputs depending on the user
- Lookup only; no search support
- Lack of standardized redirection/reference
- No standardized way of knowing what server to query
- Insecure
  - No way to authenticate the server
  - No way to encrypt data between server and client

# Chronology of gTLD RDAP Implementation [1/2]

- **19 September 2011**: SSAC's SAC 051: "*The ICANN community should evaluate and adopt a replacement domain name registration data access protocol*"
- **28 October 2011**: Board resolution adopts SAC 051
- **4 June 2012**: Roadmap to implement SAC 051 is published
- **2012**: RDAP community development within IETF WG begins
- **March 2015**: RDAP IETF RFCs are published
- **June 2015**: work on the RDAP gTLD Profile which maps RDAP features to existing policy and contractual requirements begins
- **26 July 2016**: Version 1.0 of RDAP gTLD Profile is published

# Chronology of gTLD RDAP Implementation [2/2]

- **9 August 2016**: The RySG submitted a "Request for Reconsideration" regarding the inclusion of RDAP in the Consistent Labeling & Display policy, among other things
- **1 February 2017**: A revised Consistent Labeling & Display Policy, removing the RDAP requirement was published
- **1 August 2017**: ICANN org received a proposal from the RySG with support from the RrSG to implement RDAP
- **1 September 2017**: ICANN org responded to the RySG accepting the proposal
- **25 May 2017**: The Temporary Specification for gTLD Registration Data calls for gTLD registries and registrars to implement RDAP following a common profile, SLA, and registry reporting

# RDAP Features [1/2]

**The Registration Data Access Protocol (RDAP) is a protocol designed in the IETF (RFCs 7480 - 7484) to replace the existing WHOIS protocol and provides the following benefits:**

- Standardized query, response and error messages
- Secure access to data (i.e., over HTTPS)
- Extensibility (e.g., easy to add output elements)
- Enables differentiated access (e.g., limited access for anonymous users, full access for authenticated users)

# RDAP Features [2/2]

- Bootstrapping mechanism to easily find the authoritative server for a given query
- Standardized redirection/reference mechanism (e.g., from a registry to a registrar)
- Builds on top of the well-known web protocol, HTTP
- Internationalization support for registration data
- Enables searches for objects (e.g., domain names)

# Internationalization

- Internationalized domain names supported in both the question and the answer
- Internationalized contact information is supported
- Contact information supports language tags in order to define the language / script of the data
- Replies are JSON formatted, which supports UTF-8
- The transport protocol is HTTP, which supports UTF-8

# Bootstrapping

- In the case of new gTLDs, whois.nic.<TLD> is the standard name to find the WHOIS/web-Whois server
- In the case of RDAP, the protocol defines standard bootstrap mechanism that allows a client to find the authoritative server for a particular <TLD>
- RDAP specification explains how to form direct queries and basic search queries
- http://data.iana.org/rdap/dns.json

# Thin Data in RDAP

- In a thin domain registry the domain contact information is held by the registrar. The registry RDDS only holds a referral to the registrar, the registration, expiry, creation, update date, name servers and domain status.
- A thick domain registry holds all of the contact information needed for the domain names.
- With RDAP, a Registry can point the end-user to the Registrar's RDAP in order to obtain authoritative information maintained by the Registrar.

# Differentiated Access

- Differentiated access refers to the functionality of showing different subsets of RDDS fields based on who is asking (e.g., limited access for anonymous users, full access for authenticated users)
- The Temporary Specification for gTLD Registration Data sets the basis for differentiated access by defining a minimum output and requiring contracted parties to provide access to further data on the basis of a legitimate interest
- Further policy work/requirements have to be developed in order to have a Unified Access Model that would provide for this access in a consistent way in the gTLD space

# RDAP Implementation Status in gTLDs

# Implementation Status

- The Temporary Specification for gTLD Registration Data calls for gTLD registries and registrars to implement RDAP following a common profile, SLA, and registry reporting requirements
- A proposal for a gTLD RDAP Profile ended its public comment period on 13 October 2018
- ICANN org and the contracted parties continue to negotiate an RDAP SLA and registry reporting requirements

# RDAP: Mechanism and Policy

## Specification 4

“Registry Operator shall implement a new standard supporting access to domain name registration data (SAC 051) no later than one hundred thirty-five (135) days after it is requested by ICANN if: 1) the IETF produces a standard (i.e., it is published, at least, as a Proposed Standard RFC as specified in RFC 2026); and 2) its implementation is commercially reasonable in the context of the overall operation of the registry.”

# Current Status (Temp Spec + EPDP)

Here are some RDAP implementation features potentially impacted by policy changes in ePDP and elsewhere

- Should Tech and Admin fields be treated differently? Or removed/revised?
- Should we apply different rules for legal versus natural persons?
- Will adding country codes to RDAP responses help with jurisdictional balancing test valuations?
- If we need to collect user consent for processing of a data field, do we need to change the response profile?
- When should the response profile provide a contact mechanism (anonymized email or web form) rather than original contact info?
- Should response profile include information about requesting redacted data?
  - ("Should I try the abuse contact email? Something else? Or am I out of luck?")
- How will we handle IDN variants?

- "Reasonable Access" (a term in Temp Spec) is not yet defined
- Authorization/Authentication Model is related to "Reasonable Access"; also not yet defined

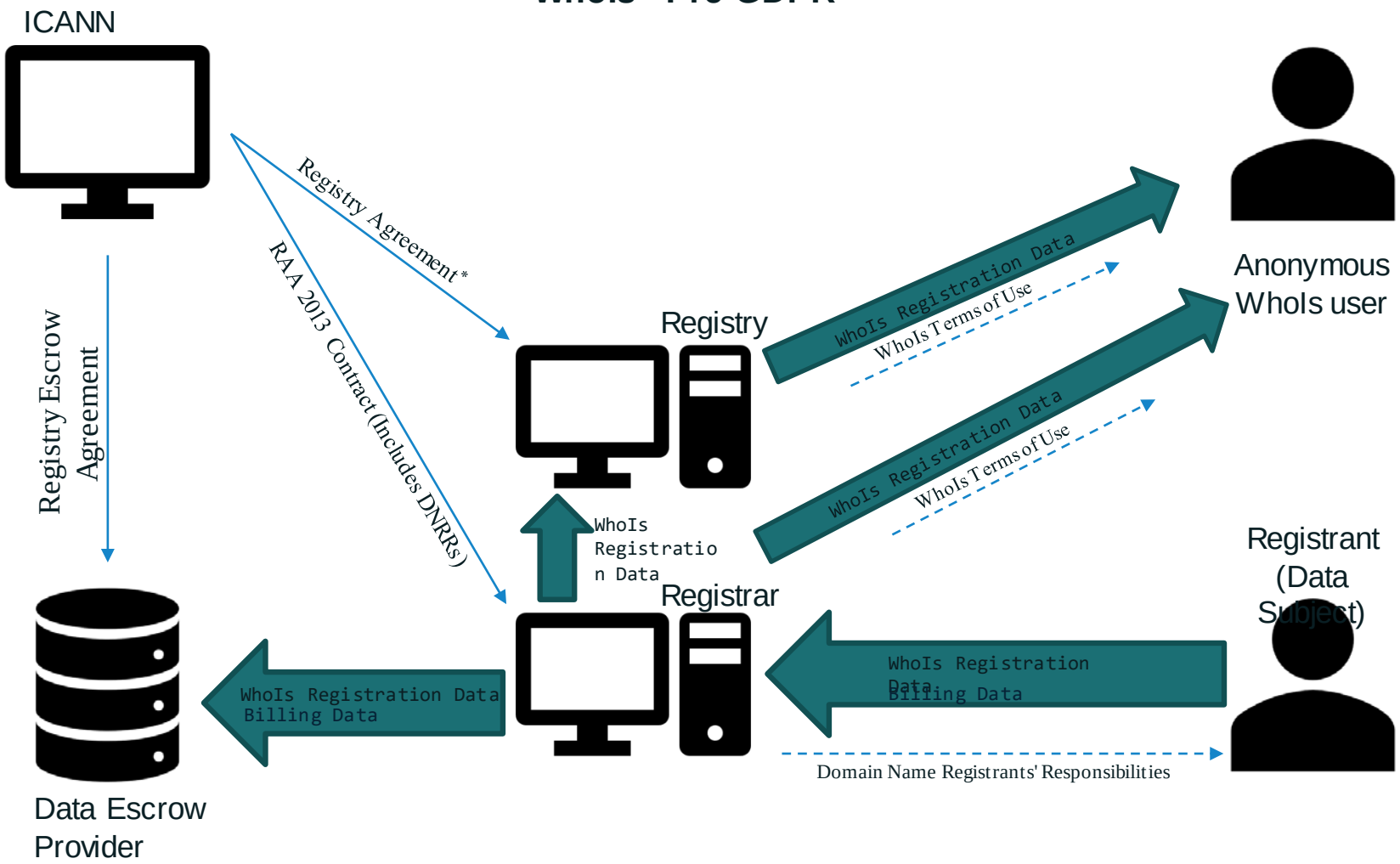
# Goals of pilot

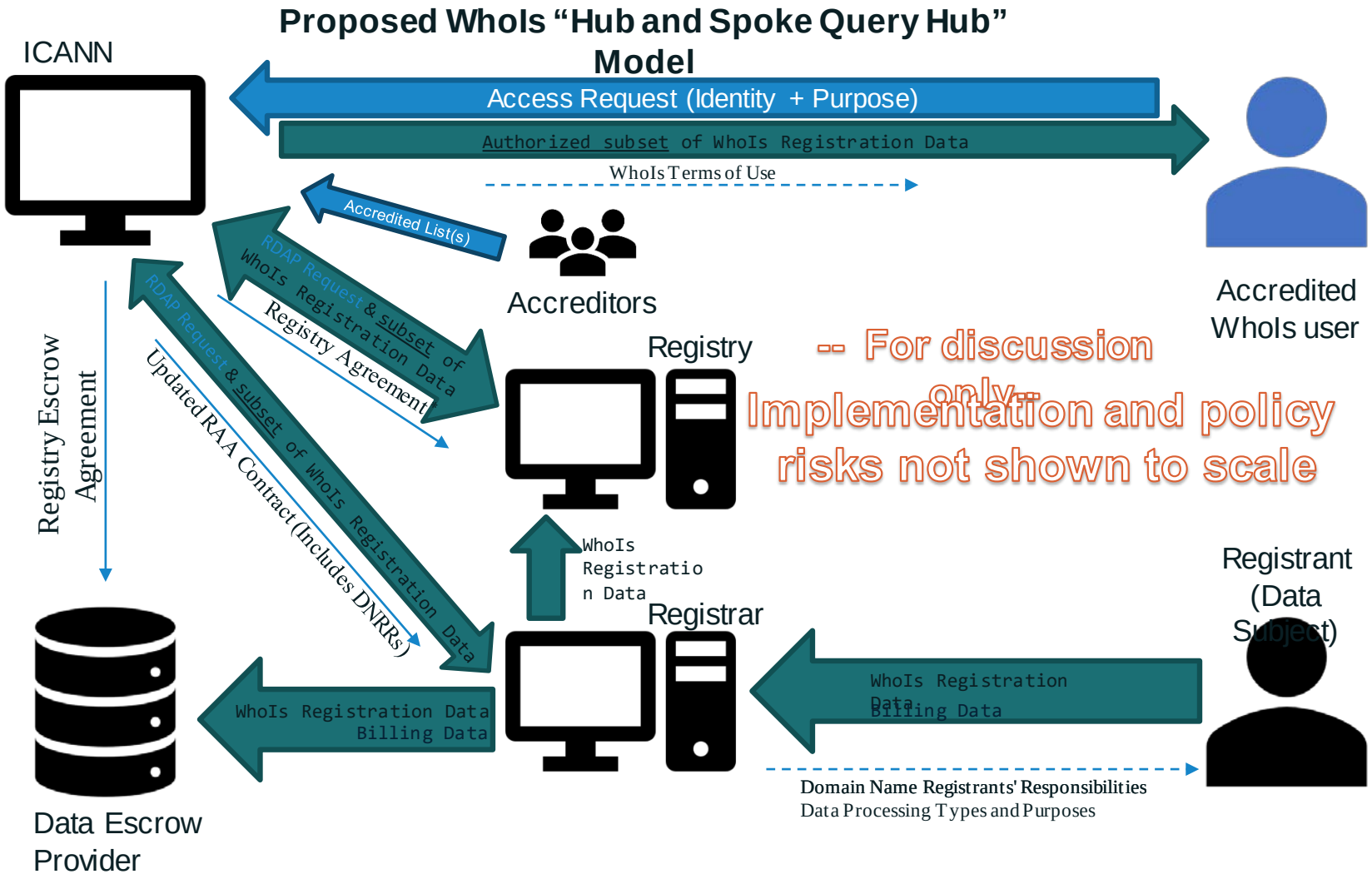
- Provide technical requirements to support provision of registration data through RDAP
- Reflect requirements in contracts and policy
- Allow experimentation with RDAP functionality
- Updated to mirror Temporary Specification as current minimum required data set

# Two Policy Development Phases

- Phase 1: Going through temp spec and determining viability/sufficiency under the new law
  - Find the bases for each type of data processed and by whom
  - Avoid discussing access models in this phase
- Phase 2: Defining access models
  - How do you facilitate the balancing test for legitimate interests required under GDPR (AKA "How does one evaluate that a request is lawful and proportionate?")
    - Accreditation
    - Authentication
    - Rights description and authorization
  - Assuming that a request is lawful, what would a response (or set of responses) look like?
    - What data are returned (fields, and sources)
    - May be different than the source data which is PII
  - How do you mitigate liability (probably not related to RDAP)?

# WhoIs - Pre-GDPR




Proposed WhoIs "Hub and Spoke Query Hub" Model
ICANN
Access Request (Identity + Purpose)
Authorized subset of WhoIs Registration Data
WhoIs Terms of Use
Accredited List(s)
Accreditors
Accredited WhoIs user
RDAP Request & subset of WhoIs Registration Data
Registry Agreement
Registry Escrow Agreement
RDAP Request & subset of WhoIs Registration Data
Updated RAA Contract (Includes DNRRs)
Registry
-- For discussion only --
Implementation and policy risks not shown to scale
WhoIs Registration Data
Registrar
Registrant (Data Subject)
WhoIs Registration Data
Billing Data
WhoIs Registration Data
Billing Data
Domain Name Registrants' Responsibilities
Data Processing Types and Purposes
Data Escrow Provider

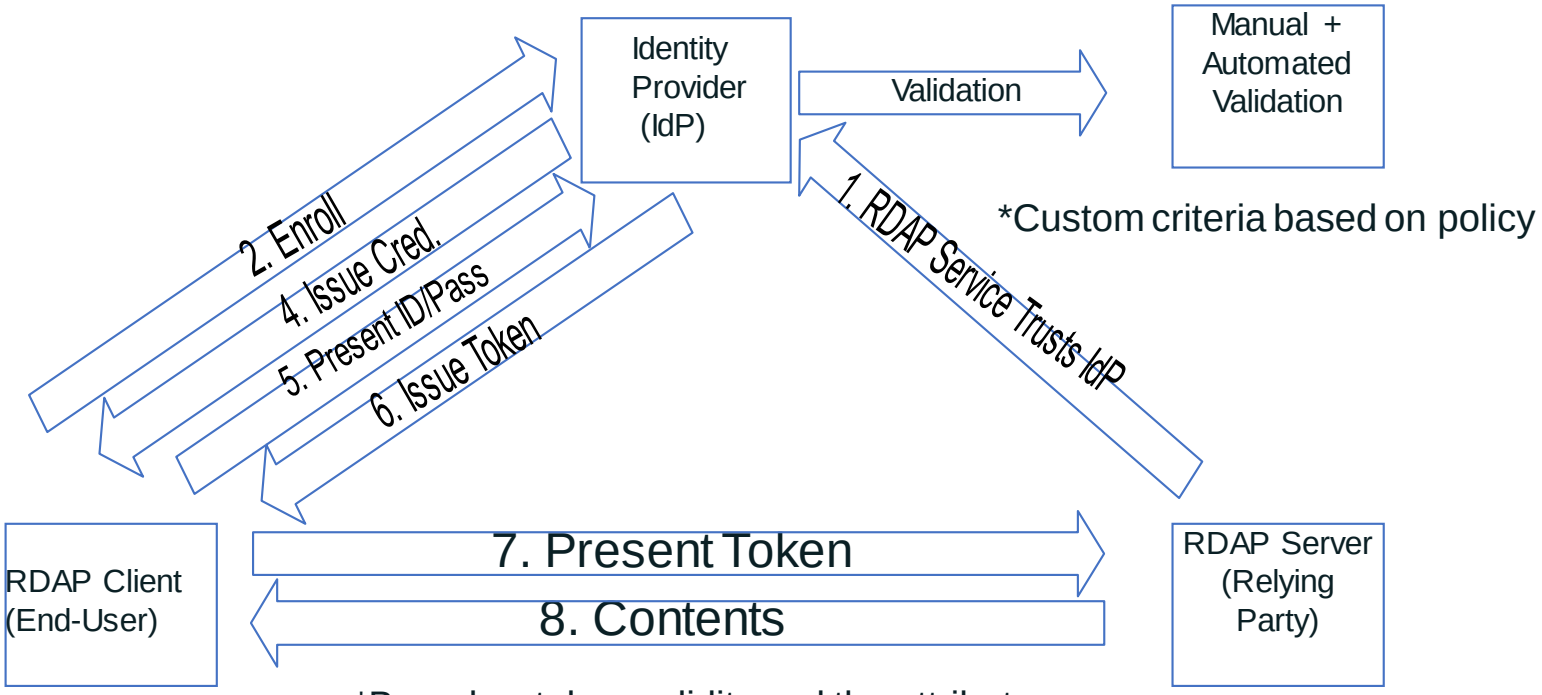
# Authentication and RDAP

# RDAP – Authentication and Access Control

**James Galvin Afilias**

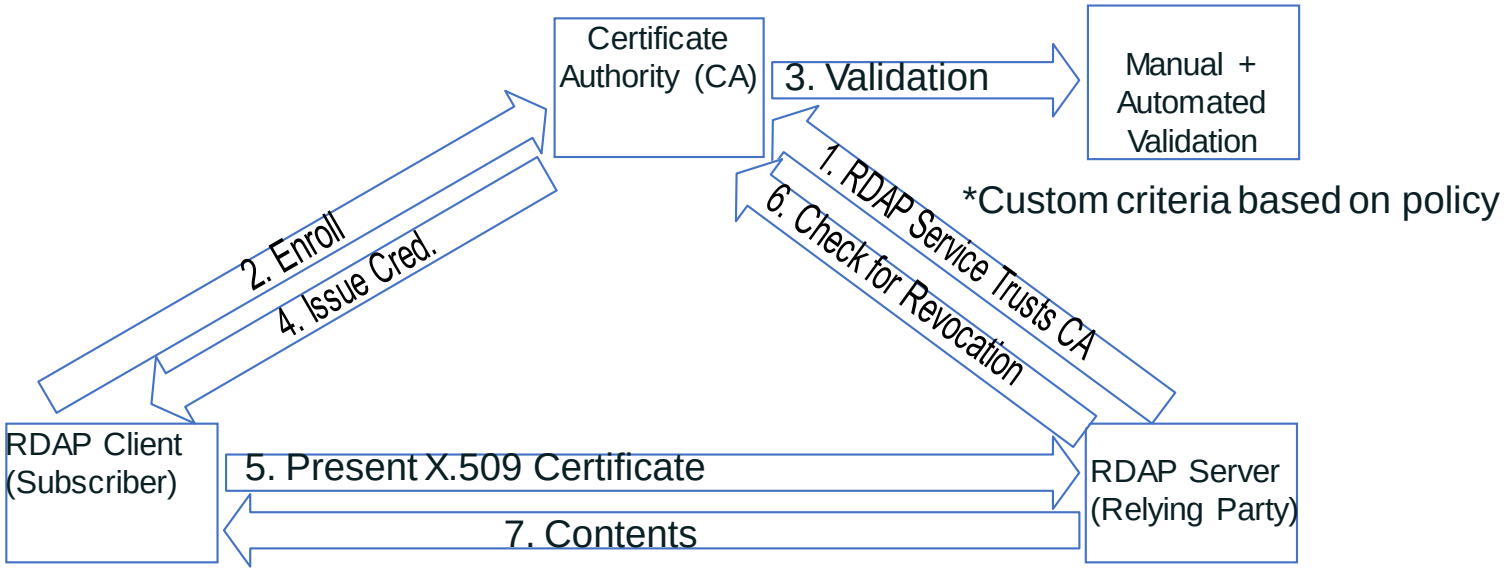
**Understanding the RDAP and the Role it can Play in RDDS Policy ICANN63 Barcelona**

# Federated Authentication High- Level Overview




ICANN

# TLS Client Authentication
# High- Level Overview




*Based on only certificate validation

ICANN

# High-Level Comparison Chart

| | Federated Authentication | TLS Client Authentication |
|---|---|---|
| **Protocol** | OAuth2.0 (rfc6749) | **TLS (rfc5246)** |
| **Layer** | Application Layer | **Transport Layer** |
| **Credential** | ID and Password | **Digital Certificate** |
| **Credential strength** | What you know | **What you have + What you know** |
| **Support accreditation based on policy** | Yes | **Yes** |
| **Support immediate credential revocation** | Yes | **Yes** |
| **Support basic access control** | Yes | **Yes** |
| **Support attribute based access control out-of-box** | Yes | **No** |
| **Tokens/credentials carry attributes out-of-box** | Yes | **Yes** |
| **Servers understand attributes out-of-box** | Yes | **No** |
| **Credential management overhead on user** | No | **Yes** |
| **Credential reissuance (Forgot/Lost Credential)** | Instant | **Moderate** |
| **Binds identity to the credential** | **No** | **Yes** |

# High-Level Comparison Chart Cont'd

| Trust (Anchor) Management | Simple | Moderate |
|---|---|---|
| **Risk of bad implementation out-of-box** | Low | **Low** |
| **Risk of bad implementation handling attributes** | Low | **Moderate** |
| **Mitigates TLS man-in-the-middle** | No | **Yes** |
| **Credential support hardware (Physical Token)** | No | **Yes** |
| **Flexibility to add attributes** | Limited | **Unlimited** |
| **Supports non-repudiation** | No | **Yes** |
| **Implementation lead time** | **Short** | **Long** |

ICANN

# Observations

- These two technologies do not collide, both can be used if desired or necessary. The balance between convenience and security needs to be considered.
- Key difference is the quality of accountability – binding the identity of the user to the credential.
- A hybrid model may be most appropriate.

ICANN

# Thanks

Special thanks to Tomofumi Okubo, Digicert, for the protocol diagrams and comparison charts: http://regiops.net/wp-content/uploads/2018/05/7-ROW7_Auth_Comparison_TO_051718_2.pdf

# Registrar Perspectives on RDAP

# Registrar Perspective

- Operational Efficiency
  - Port 43 IP whitelists replaced by either SSL whitelist or centralized authorization system.
- Universal Acceptance
  - Port 43 standard only supports ASCII characters
  - Inconsistent display among WHOIS clients for UniCode characters
  - RDAP enables multiple scripts to be transmitted so that the Registrant/User could be able to view the data in their native or preferred script
- Consistent Data Structure

ICANN

# RDAP Client Demo

# Engage with ICANN

## Thank You and Questions

Visit us at **icann.org**
Email: globalSupport@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg