IANA Update for the ccNSO

Kim Davies
VP, IANA Services & President, PTI

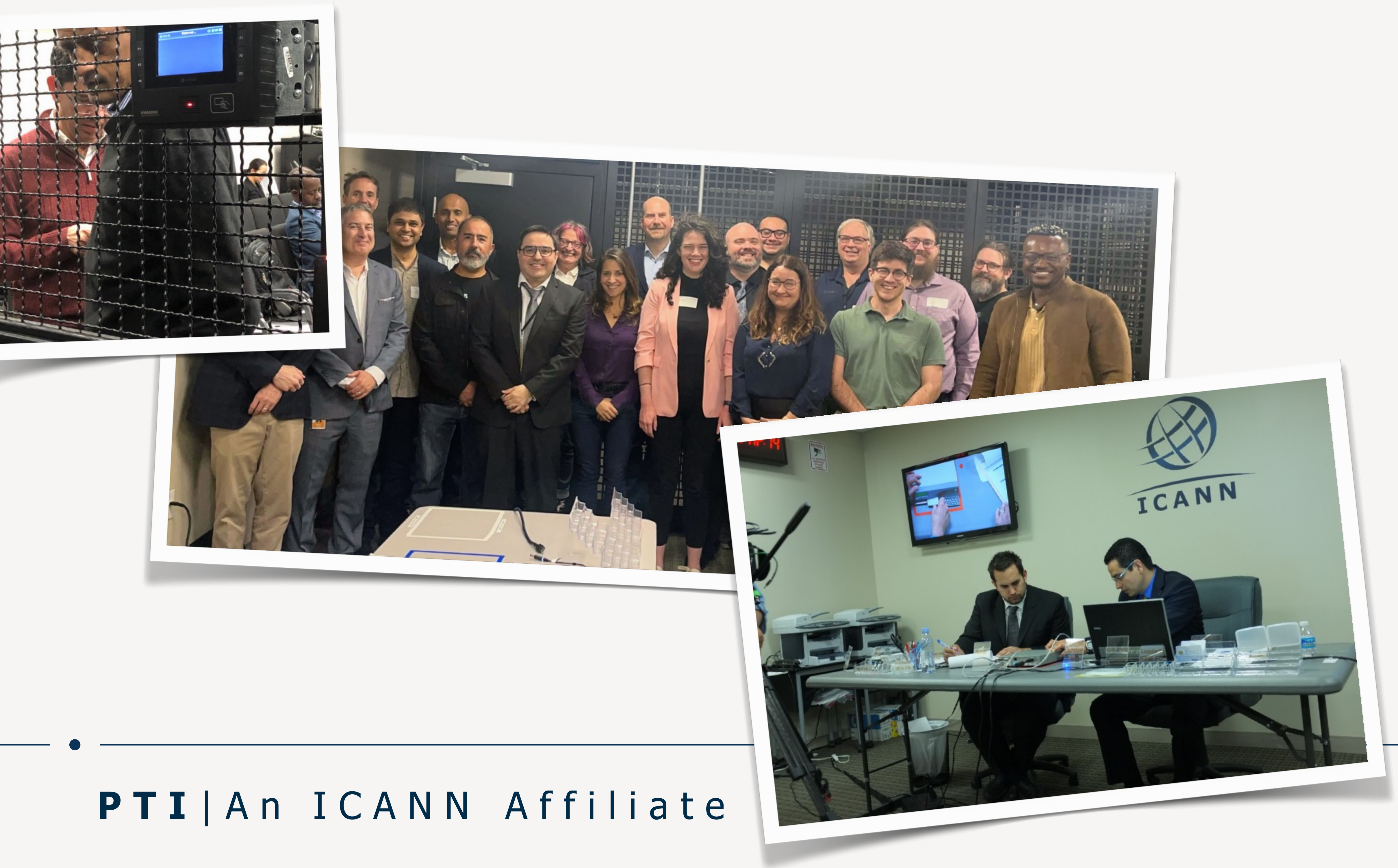
Istanbul
November 2024

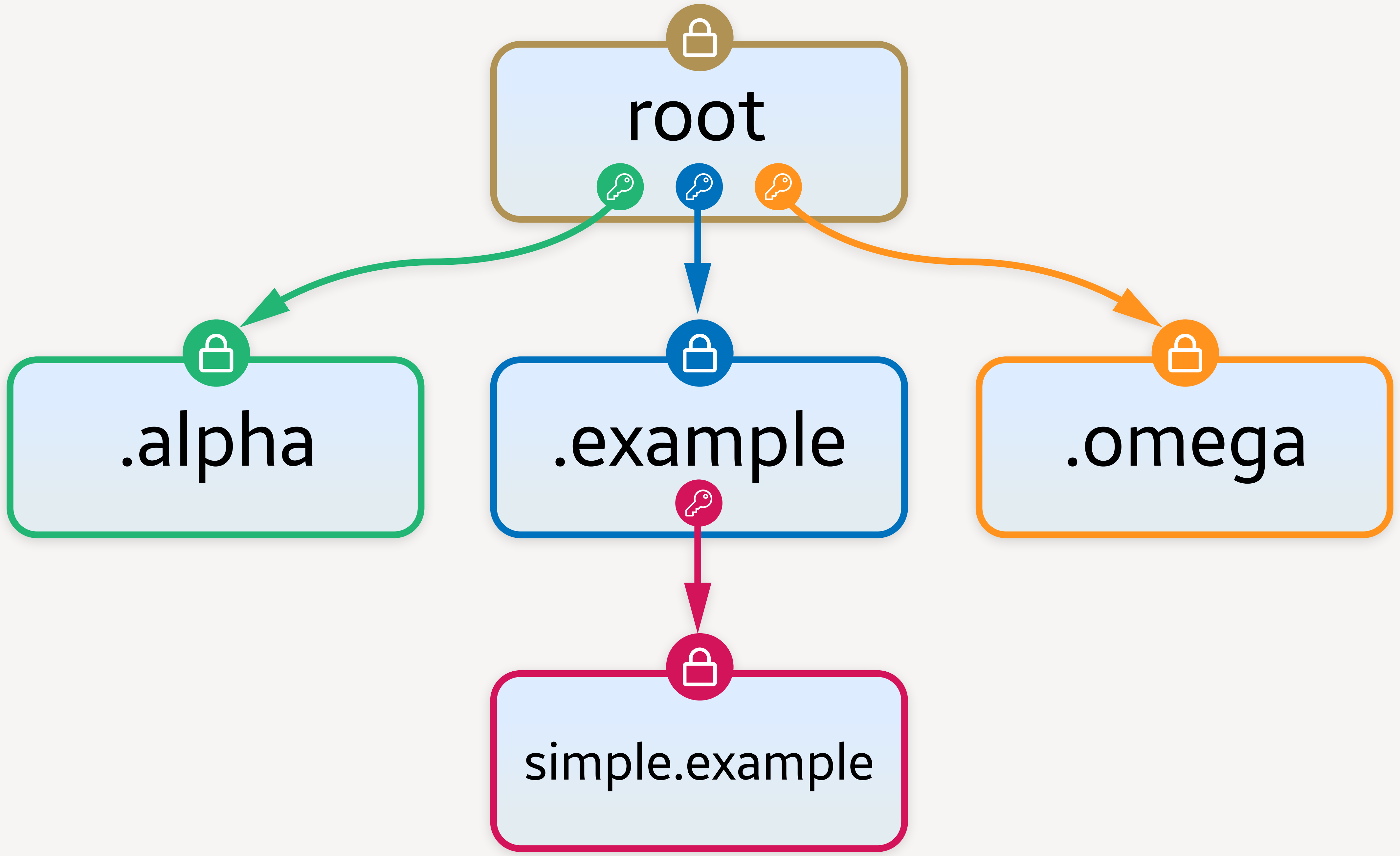
PTI | An ICANN Affiliate

ICANN 81 ANNUAL GENERAL MEETING

DNS Trust Anchor

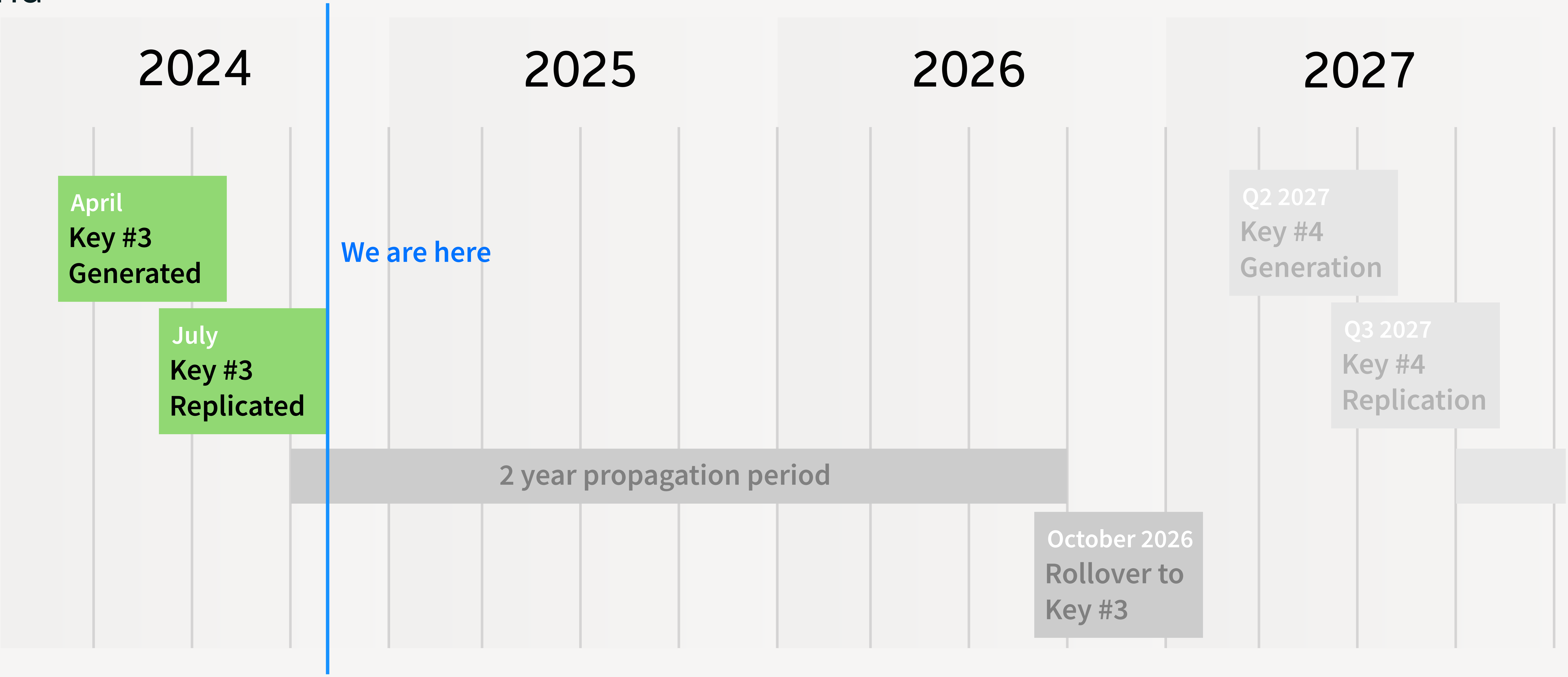
- Security for the DNS (DNSSEC) is a hierarchical system of public key cryptography that matches the hierarchical delegation of the DNS itself.
- The apex key is the **Root Zone Key Signing Key (KSK)**, which serves as the singular trust anchor for the system.
- We manage the key in a highly transparent manner, with public key signing ceremonies and an open design model.





Updating the key

- We've embarked on the 2nd ever replacement of the key
  - Highly orchestrated event, propagation to all validators through vendor updates etc.
  - Delayed due to (a) COVID, and (b) key hardware vendor change; but now underway
- Implements a 3 year cadence, with new algorithm potential in 2027 and beyond



Now available

- The new trust anchor is now available for propagation (XML file)
  - Most users will adopt it naturally through software updates
  - Will appear in the DNS itself starting 11 January 2025

Key Status

This table provides additional guidance on how keys have been issues and used. Software implementers should rely on the XML trust anchors file for normative parameters on keys.

INFORMAL NAME	STATUS	DETAILS
KSK-2024	Pre-Publication	Generated 2024-04-26 (attestation) with key tag 38696 and label Kmyv6jo. Expected to be published in DNS on 2025-01-11, and actively signing starting 2026-10-11.
KSK-2017	Active	Generated 2016-10-27 (attestation) with key tag 20326 and label Klajeyz. Signing since 2018-10-11.
KSK-2023	Abandoned	Generated 2023-04-27 (attestation) with key tag 46211 and label Kmrfl3b. Will not be used, superseded by KSK-2024.
KSK-2010	Retired	Generated 2010-06-16 (attestation) with key tag 19036 and label Kjqmt7v. Signing between 2010-07-15 and 2018-10-11.

https://iana.org/dnssec/files

Multi-factor authentication

- **Now available as an opt-in feature**
- Extra layer of protection for access to IANA's Root Zone Management System by authorized representatives of TLD managers.
- Uses standards-based TOTP approach (e.g. 6-digit rolling code authenticator app)
- Recovery codes provided as a backup
- Loss of credentials require re-proving your identity to IANA staff

Customer Identity Program

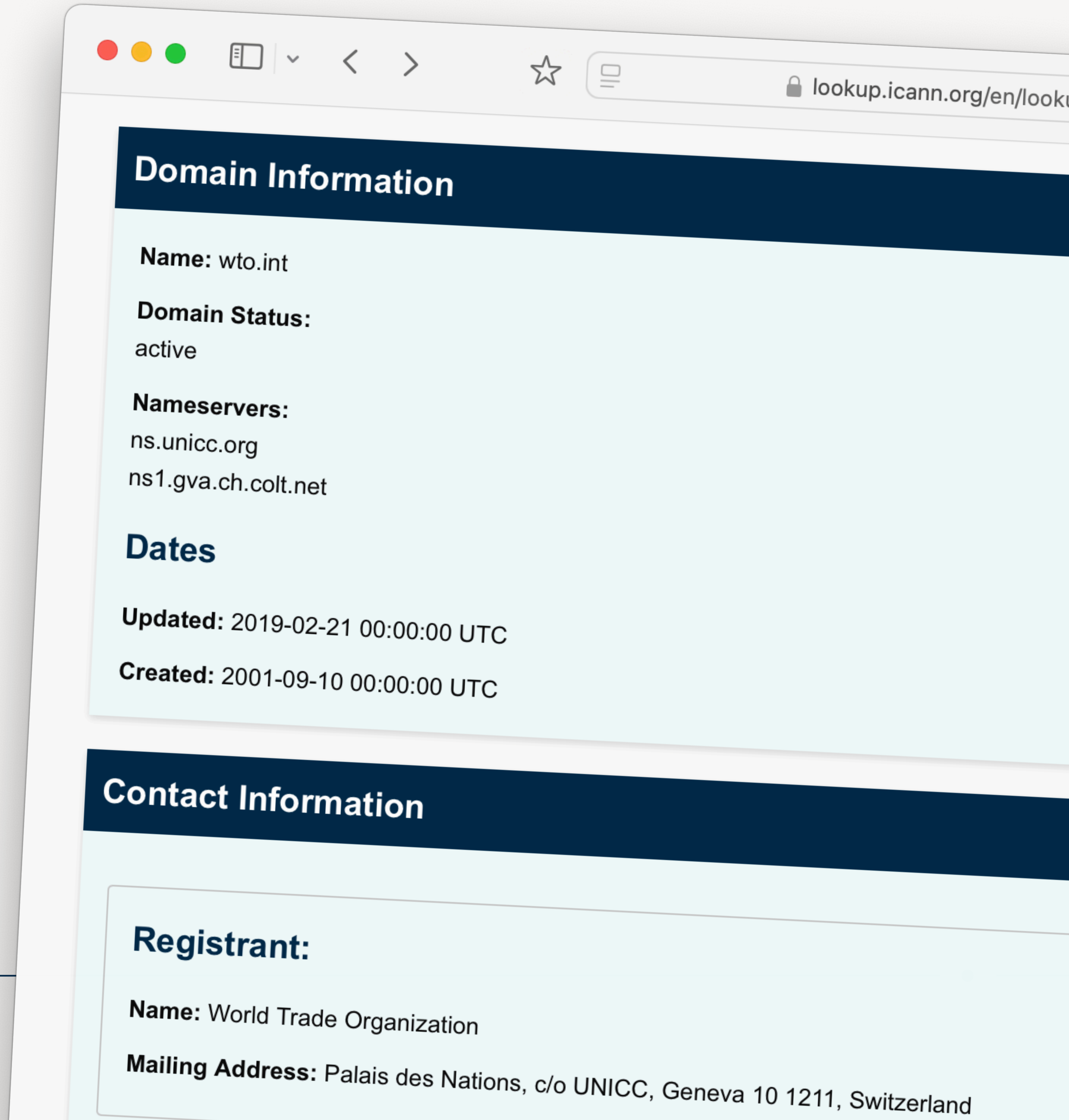
- Historically, IANA has not known who all our customers are
  - Prevalent use of “role accounts” due to the shared roles with the public WHOIS data
- Seeking to establish the natural identity of all of our customers
  - Allows re-establishment of trust in the event of credential loss
  - Compliance benefit
- **Currently optional, but required to enable multi-factor authentication**
- 3rd-party provider validates identities with government issued ID and lividity tests through web or app
  - e.g. similar to some checks for online boarding pass collection
- IANA staff do not see or retain identity documents, only the results of the tests

API Enhancement

- The RZMS API allows users to create, view, approve, and withdraw change requests via API call
  - Ideal for facilitating bulk actions.
- API tokens managed from within the RZMS account.
- Ability to create, revoke, and track token usage]
- Operational Test & Evaluation (OTE) Environment to test API actions before executing in production
  - OTE Data is refreshed periodically
  - No emails are sent from the OTE environment
  - No copy of the root zone is made available from the data in the OTE environment.

RDAP

- IANA has launched its own RDAP server at rdap.iana.org
  - Incremental roll-out
  - Initially limited to .INT domains
  - Intended to cover all IANA resources like our WHOIS server (e.g. root zone entries, reverse DNS, IP address allocations etc.)
  - Unintended consequences for listing our “root” repository even though the RFC specifically allows for it, due to client behavior
- Don’t forget to list your RDAP server in the root zone
  - List in RZMS as a usual root zone change request
  - Approved changes will be propagated through “bootstrap” registry
  - Bootstrap registry is used by RDAP clients to find RDAP servers

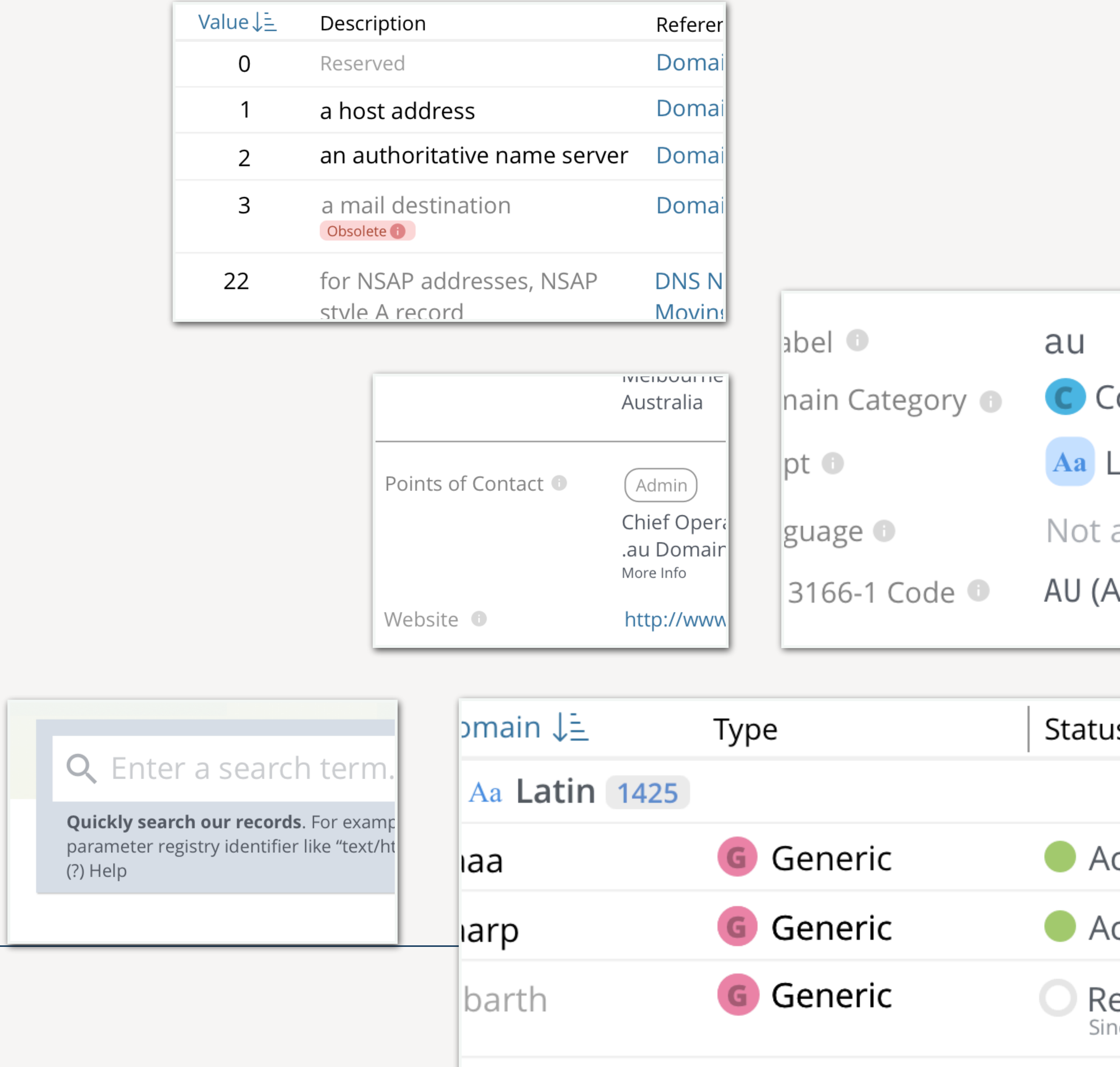


Next steps in RZMS Development

- Reducing friction in the change request workflow by allowing users to dismiss low-priority technical issues, e.g. serial number consistency, without requiring involvement from IANA staff.
- Updates to the authorization policies based on community feedback, including new policies allowing TLD managers to grant their providers autonomy in managing KSK rollovers.
- Passwordless authentication using newer web authentication standards (e.g. passkeys).
- Variant implementation
  - Outputs of PDPs from GNSO and ccNSO
- Name Collision Assessment for next round of new gTLDs

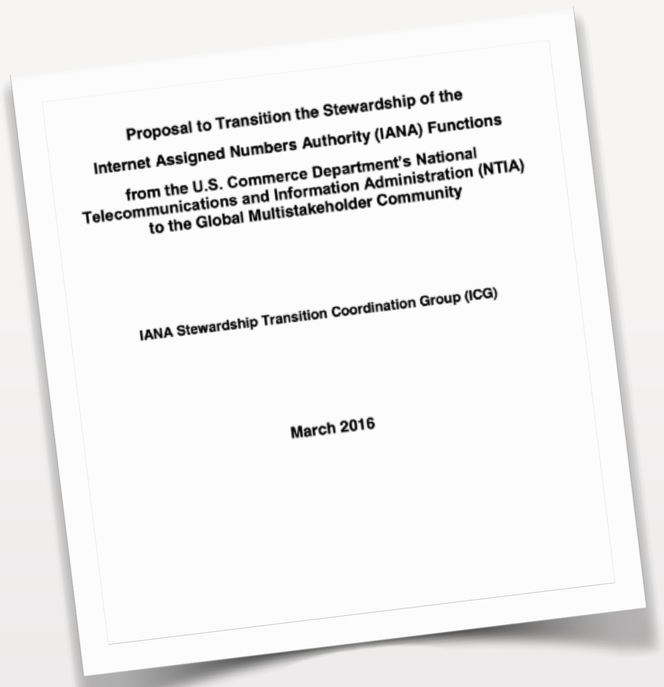
Website and brand enhancements

- IANA is reviewing how to better present data on its website
  - Modern navigation and design
  - Surface useful material that is currently buried
  - Better data navigation
  - Share new data that is currently collected but not published
  - Machine-readable formats



Where should IANA be in 2030?

- Both ICANN and IANA are developing our next five year strategies
  - Where do we want to be in 5 years?
  - What does the community want to evolve?
- Consultations will commence later this month


Proposal to Transition the Stewardship of the
Internet Assigned Numbers Authority (IANA) Functions
from the U.S. Commerce Department's National
Telecommunications and Information Administration (NTIA)
to the Global Multistakeholder Community

IANA Stewardship Transition Coordination Group (ICG)

March 2016

- Implement the IANA stewardship transition

2016-2020

- First dedicated IANA strategy
- Five focus areas
- In its final year

2020-2025

?

2025-2030

We need your ideas on engagement

- We perform an annual engagement survey of our customers and community.
- Its very short (<5 minutes) and provides us insights on how to improve, particularly with feedback on FY26 engagement activities:

Thank you!

kim.davies@iana.org