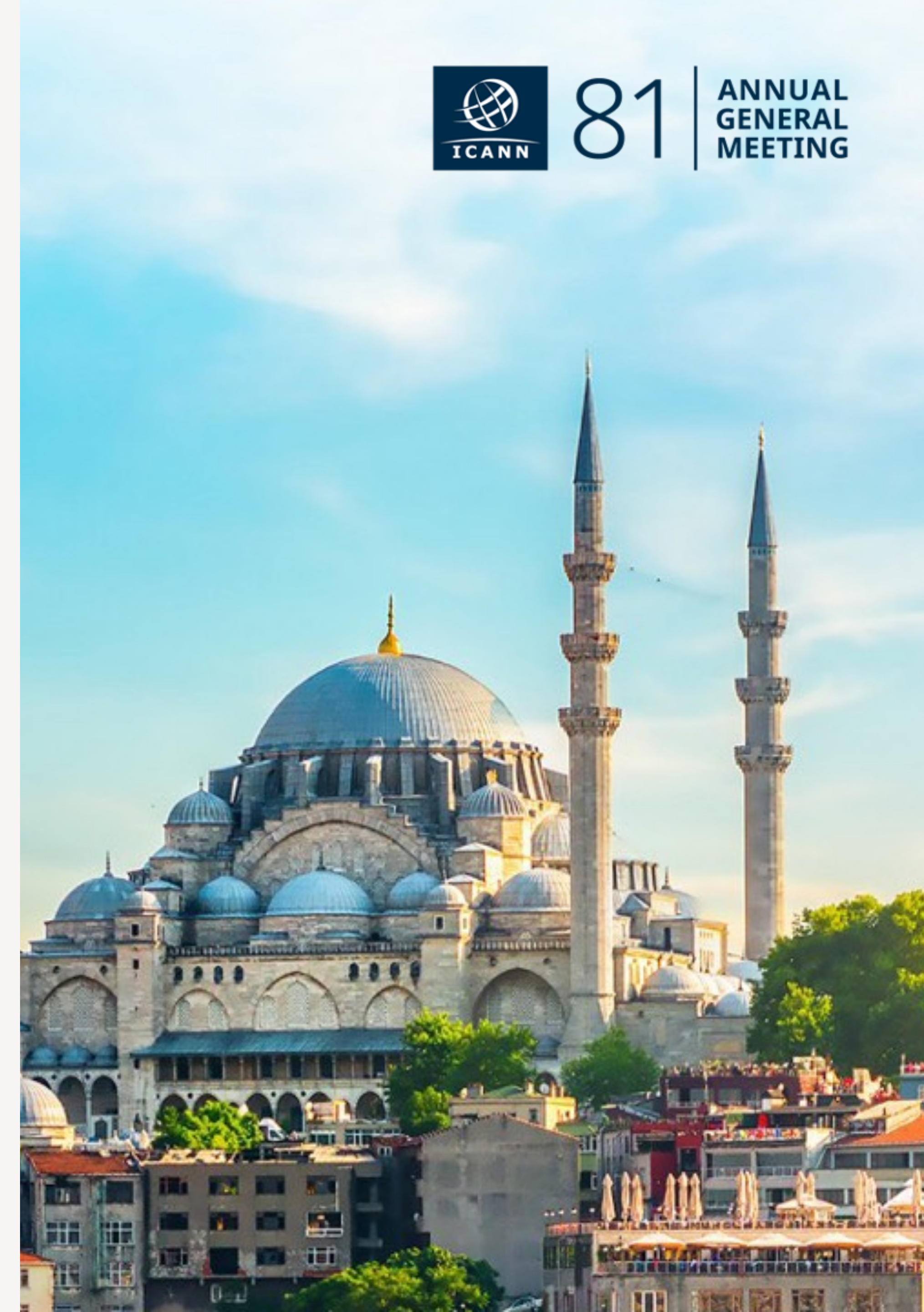# IANA Update for the GNSO

Kim Davies
VP, IANA Services & President, PTI

Istanbul
November 2024

PTI | An ICANN Affiliate

Agenda

- Updates in the DNS Trust Anchor
- .INTERNAL
- Multi-factor authentication
- Customer Identity Program
- API enhancement
- RDAP
- Next steps in RZMS development
- Next round
- Website/brand redesign
- IANA in 2030 (our next strategic plan)
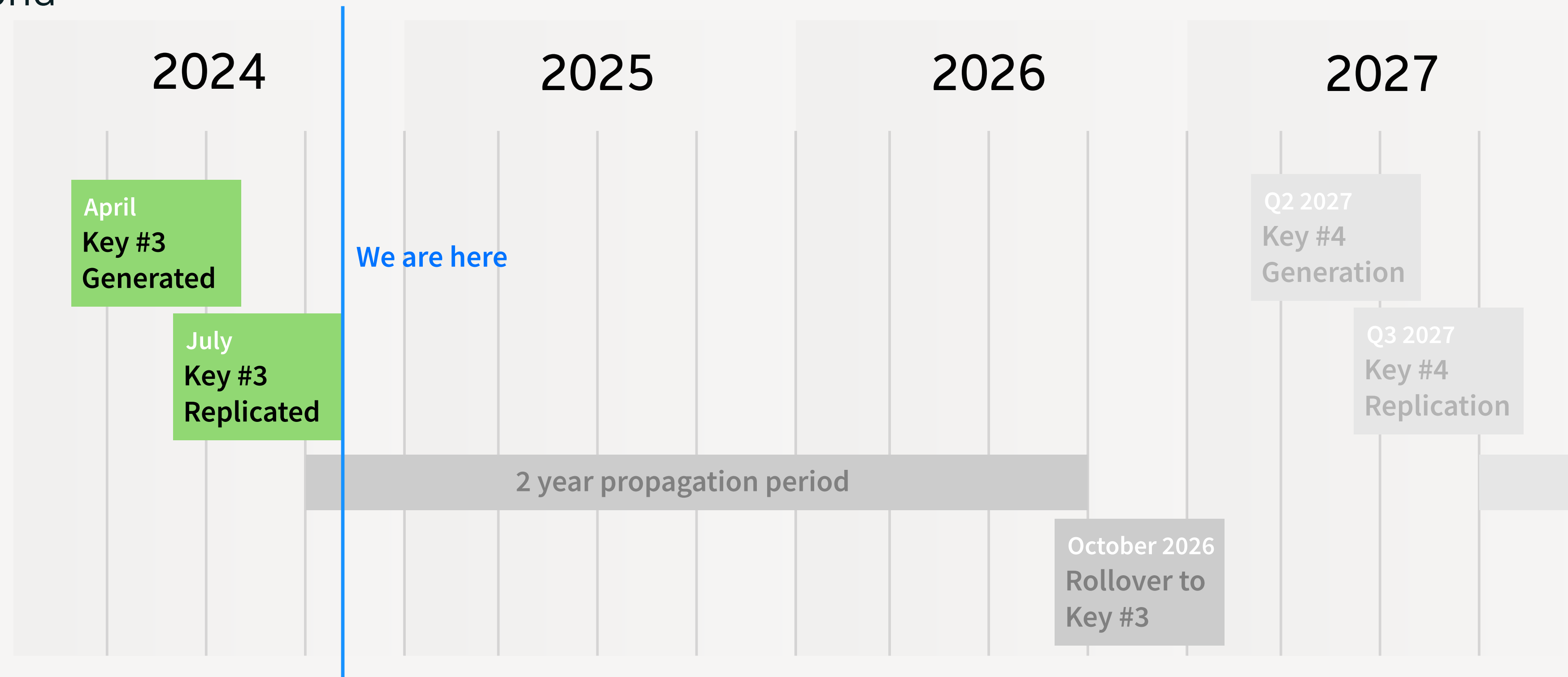- Engagement Survey

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.
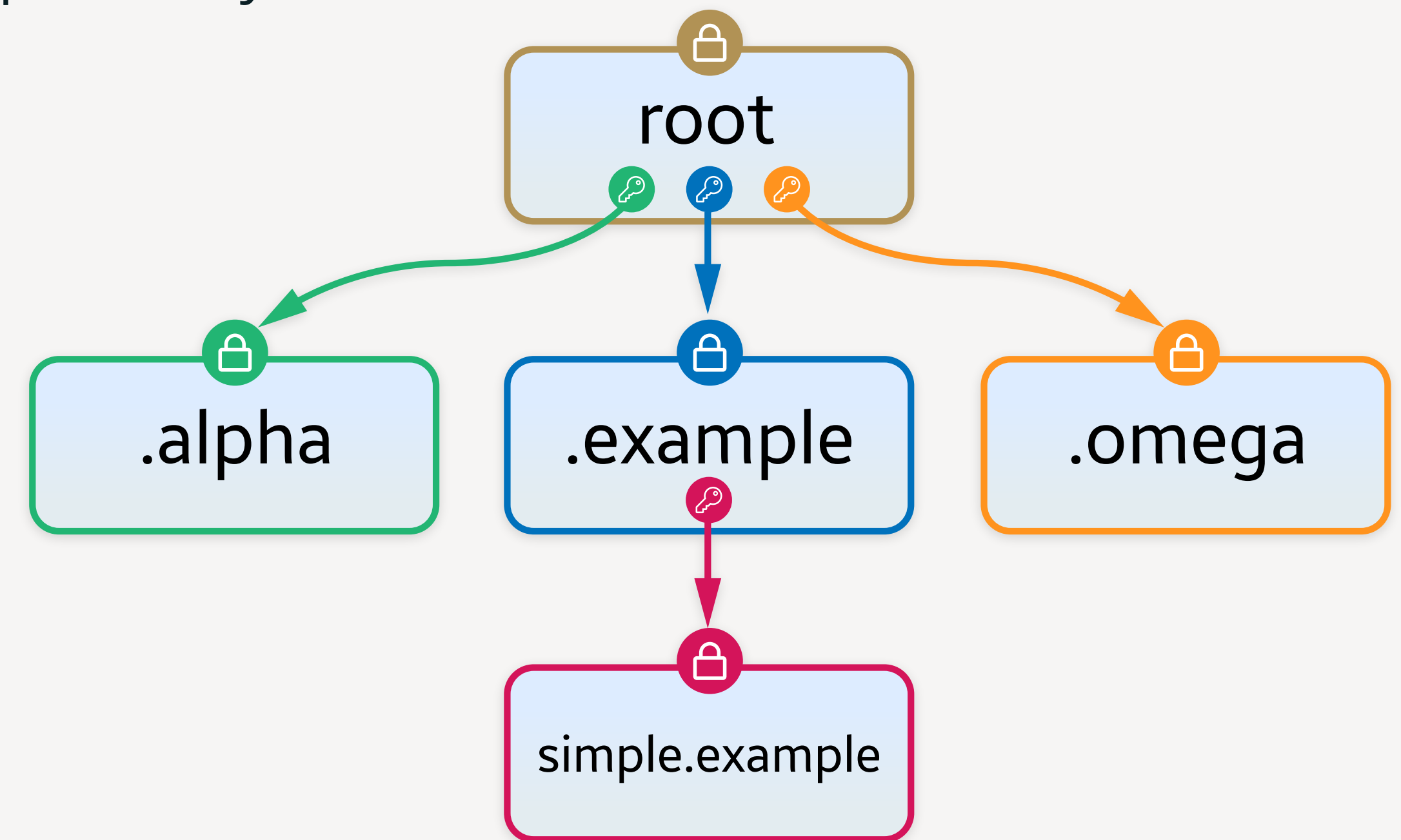
Updating the key

- 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

2024	2025	2026	2027

April
Key #3 Generated

We are here

July
Key #3 Replicated

2 year propagation period

October 2026
Rollover to Key #3

Q2 2027
Key #4 Generation

Q3 2027
Key #4 Replication

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

.INTERNAL

- Recently reserved for use in private networks
    - DNS equivalent to RFC1918 address space
- Will not be provisioned in the global DNS to avoid conflicts
- Compare and contrast with
    - .local — multicast DNS
    - .alt — alternate resolution techniques
    - .home.arpa — home network control protocol
- Internet Draft under development
    - https://datatracker.ietf.org/doc/draft-davies-internal-tld/

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
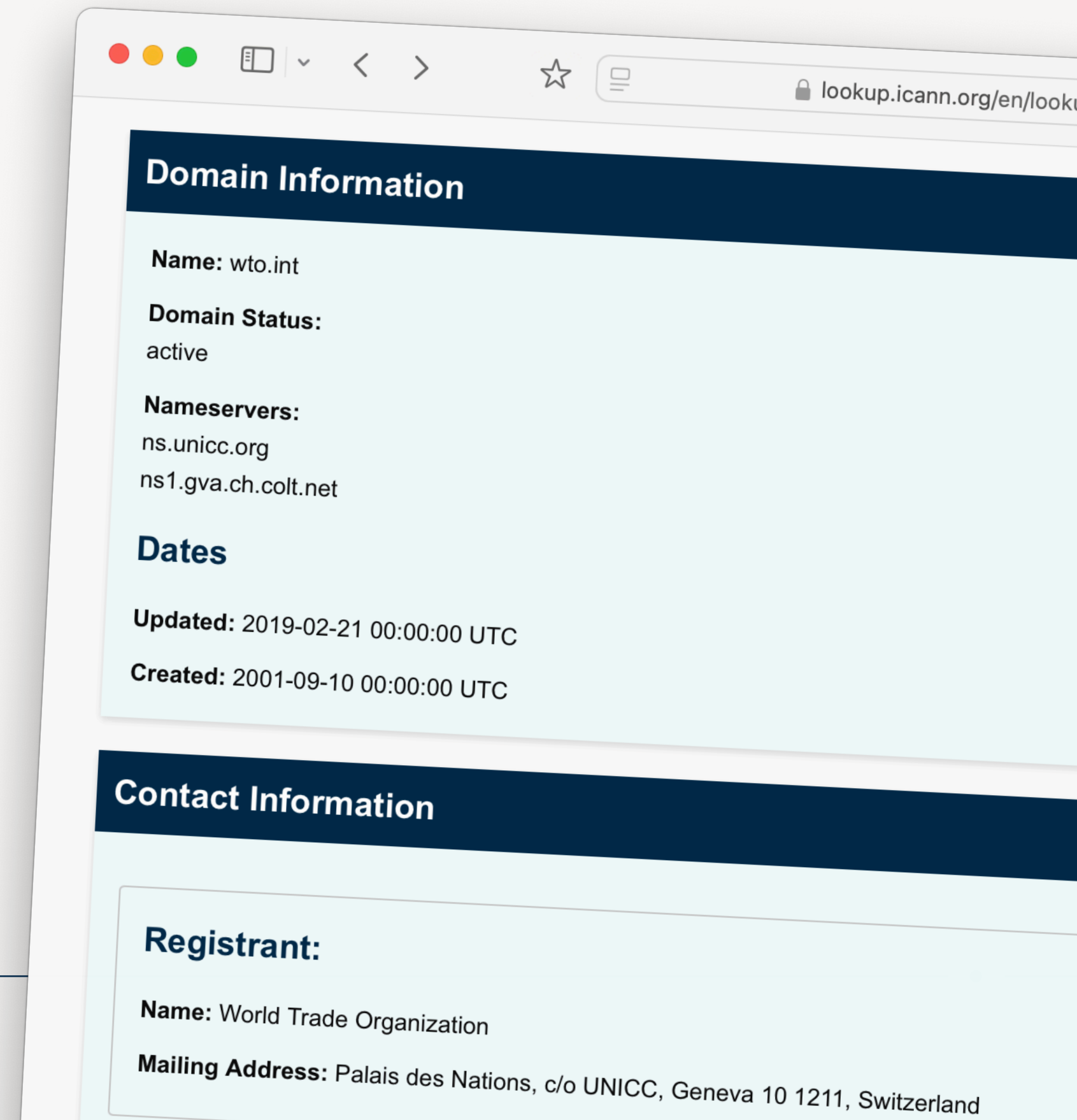
API Enhancement

- 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.

```
-  "technicalContact": {
      "name": "string",
      "organizationName": "string",
    + "address": { … },
      "email": "string",
      "phone": "string",
      "fax": "string"
  },
-  "nameServers": {
    + "add": [ … ],
    + "update": [ … ],
    + "remove": [ … ]
  },
-  "trustAnchors": {
    + "add": [ … ],
    + "remove": [ … ],
    + "replace": [ … ]
  },
-  "rdapServers": {
    + "add": [ … ],
    + "remove": [ … ],
    + "replace": [ … ]
  },
  "whoisServer": "string",
```

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

lookup.icann.org/en/looku

Domain Information

Name: wto.int

Domain Status:
active

Nameservers:
ns.unicc.org
ns1.gva.ch.colt.net

Dates

Updated: 2019-02-21 00:00:00 UTC

Created: 2001-09-10 00:00:00 UTC

Contact Information

Registrant:

Name: World Trade Organization

Mailing Address: Palais des Nations, c/o UNICC, Geneva 10 1211, Switzerland

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).

Next Round of New gTLDs

- IANA is largely not involved in the evaluation of applications
  - Applicant Guidebook is designed to be a superset of IANA requirements
- NCAP policy proposes piloting delegations in the root zone in order for technical review team to collect data
  - Involves developing new business processes in IANA (high impact)
- IANA is involved in delegations
  - Responsible for administering change rate policies
  - Expected to model on how 2012 round was performed
  - Impact of variants in a potential big impacts on delegations and beyond
- Estimating first delegations around in mid to late 2027

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
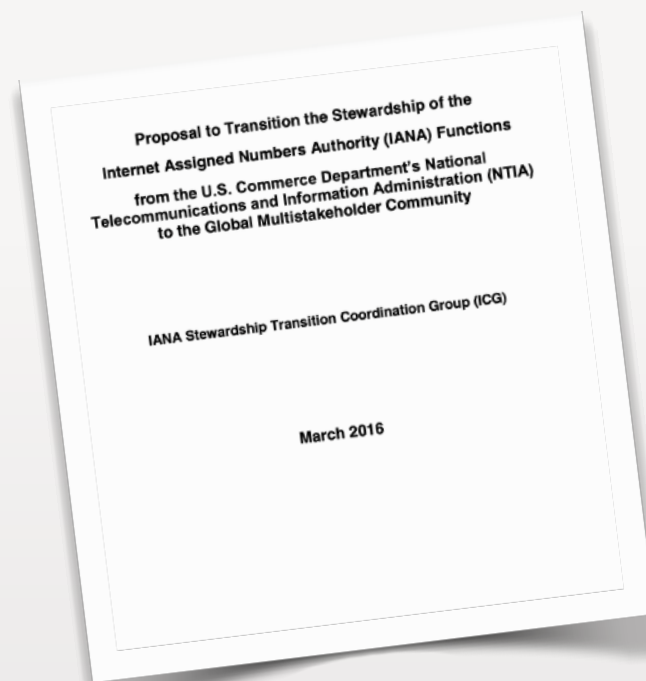
- Implement the IANA stewardship transition

2016-2020

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

2020-2025

?

2025-2030

Regroup on the past 5 years

- Generally successful in meeting ambitions
- Consistent delivery of the IANA functions
- Product delivery was not as fast as estimated
  - Lack of development resources key contributing factor
- Expanding engagement objectives were limited
  - COVID was a key contributing factor
- Managed to implement a number of initiatives to simply arrangements from the IANA stewardship transition
  - Planning timelines were synced with ICANN
- Project management improvements
- New concerns have arisen
  - Transactional volume increases
  - Lack of coverage and redundancy in staff

PTI|An ICANN Affiliate

PTI **STRATEGIC PLAN**

July 2020 - June 2024

Identified objectives for next 5 years

- **Innovation**
  - Our main goal is to enhance our agility and reduce time-to-market for new features, allowing IANA to adapt quickly to technological advancements and evolving customer needs.

- **Operational Excellence**
  - We will focus on staff development, streamlining processes, and evolving continuous improvement best practices.

- **Community Engagement**
  - Our main objective is to maintain our relationships with community leaders, and improving communication strategies targeted at non-traditional stakeholders.

PTI|An ICANN Affiliate

IANA 2030 STRATEGY

The Public Technical Identifiers (PTI) Strategic Plan covering July 2025 to June 2030

September 2024 Draft, For Public Review

Consultation on plans

- **Strategic Plan**
  - "IANA in 2030" session on Monday afternoon
  - Proceeding opens 26 November
    - Closes 29 January 2025

- **Operating Plan and Budget**
  - IANA is also consulting on its annual operating plan and budget
  - Proceeding opens 17 December
    - Closes 17 February 2025
  - Simultaneous consultation on ICANN, IANA and PTI OP&B
  - Community webinars in mid-December

- **Key stakeholder input is essential**

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