IANA Update

Kim Davies
VP, IANA Services; President, PTI

September 2024

PTI | An ICANN Affiliate

Topics

- Root Zone Operations
  - Evolving Authentication and Authorization
  - Our second KSK rollover
  - Updating to new DNSSEC cryptographic algorithms
- .INTERNAL domain
- Next round of new gTLDs
  - Name Collisions
  - Variants
- Machine readable registries

Evolving authentication and authorization for the root zone

To date

- Open contact models descendent from InterNIC
- Administrative and Technical contacts
  - Published
  - Responsible for cross-verifying subsequent change requests
  - Admin contact must be in country for ccTLDs
- Significant change in late 2022
  - Public contacts no longer have an intrinsic role in approvals
  - TLD managers can now configured users in our system, with granular access control
  - Approval thresholds can also be configured

Enhancing account security

- Trust model appears at first glance to be insufficient
  - Until recently, presenting tokens emailed to contacts
  - Since 2022, username/password based authentication
  - For critical infrastructure, is this enough?
- Operational procedure for the root zone also requires you demonstrate control of the zone file
  - NS, DS record changes in the root zone need to first be reflected as changes in the TLD zone
  - “Root Zone Update Process Study” (2022) concluded “… does not believe requiring the use of multi factor authentication will materially improve the security of the system when viewed in its entirety”
- ICANN 2nd Security and Stability Review (2021): “… accelerate the implementation of … security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.”

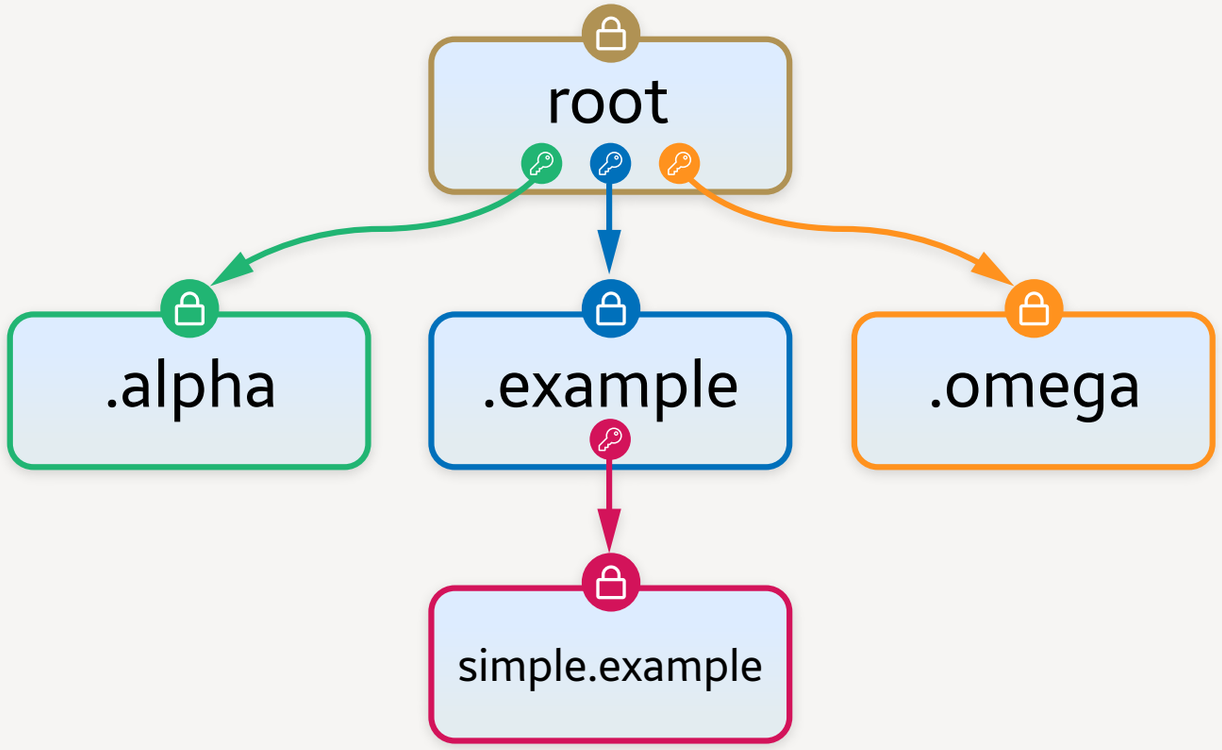
Multi-factor authentication

- Rolling out multi-factor authentication by end of year
  - Opt-in
  - Initially: TOTP (RFC 6238) (i.e. authenticator app with 6-digit rolling code)
  - Roadmap item: Passkeys
  - No telephony based authentication/recovery
- Majority of work has been relating to Know Your Customer (KYC) procedures
  - User accounts associated with individuals, not roles
    - Establish identity of the users
      - Primarily to aid account recovery
    - Using a third-party identity verification provider
      - IANA retains minimum PII and not the identity documents
- Existing measures still stay in place
  - Prove ability to edit TLD zone for root zone changes

Our second KSK rollover

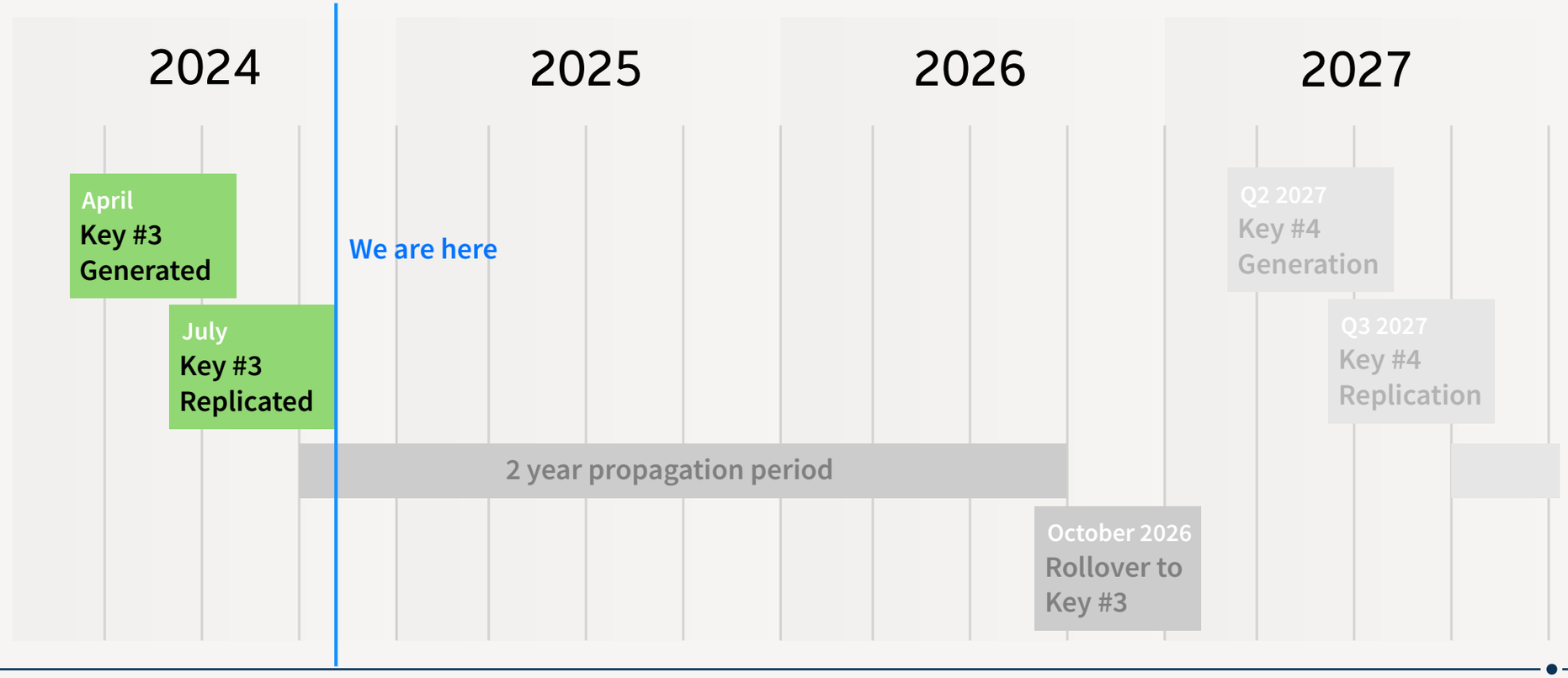
DNS Trust Anchor

- 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
  - Aim is to have a predictable routine
  - Early propagation gives large window a quick rollover could be used in emergency



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.

Updating cryptographic algorithms in the root zone

To date

- Root Zone started to be signed in 2010 using RSA/SHA-256
- Root Zone still signed with RSA/SHA-256
- Need to maintain agility to change algorithm
  - Elliptic curve algorithms (e.g. ECDSA) may give significant benefits (reduced signature size)
  - Ability to be responsive to future flaws in algorithm
- The root zone is often “special” in implementations therefore special care is needed in how to do this
- ICANN convened a community design panel to develop recommendations on how the algorithm could be changed
  - Final report issued in mid-2024
  - 26 recommendations to guide operationalization of algorithm changes

Next rollover

- “Recommendation 26: The community should prepare to be operationally ready for a root zone algorithm rollover. The next logical time for this is following the second KSK rollover, in approximately five years.”
- Essentially implementation would involve an assessment of candidate algorithms every 3 years, at the commencement of each rollover cycle.
- According to the idealized schedule
  - October 11, 2026 — rollover to next RSA/SHA-256 trust anchor
  - April 2027 — generate the next key
  - October 11, 2029 — rollover to the subsequent key (maybe new algorithm)
- Therefore, assessment of algorithms and having systems and tools operationally ready within IANA needs to happen prior to April 2027.
  - Expect it to be a significant activity in our FY26 (i.e. July 2025 onward)

.INTERNAL

A private-use TLD

- Various suggestions emerged in the community
  - Desire to have something comparable to RFC1918 private use IP address space
  - Unfettered address space for use within private networks without constraint
  - Internet Drafts in the IETF etc. raised questions about whether this was IETF work (technical protocol) or ICANN work (namespace decision)
- ICANN Security and Stability Advisory Committee issued SAC113, calling for ICANN to reserve a single string for these purposes
- ICANN consulted carefully on what the implementation procedure should be
  - Two period of public consultation
    - What the evaluation process should be
    - Validating the outcome of the evaluation process met the criteria
  - Recognized there was a lot of opinion and personal preference, sought to make the process as objective as possible

Evaluation procedure

- IANA conducted a lightweight assessment of candidate strings against the 4 assessment criteria defined in SAC113
- Tested meaningfulness and confusability using a structured approach, including reviewing in the 6 UN languages
- Not exhaustive, nor a beauty contest
  - Criteria is _a_ string that meets the SAC113, not the “best” string — which is subjective and unlikely to yield any consensus

Preliminary internal worksheet on candidate string attributes

SAC113 Candidate String Evaluation Inputs

Candidate String	String Language	Length (U-label)	Length (A-label)	Meaningful (adequately self-documents its property as a private-use space)						No alternate
				EN	AR	ZH	FR	RU	ES	EN
Contributed candidates										
	EN	8	8	✔						✔
	EN	10	10	✔						✔
	EN	7	7	✔						✔
	—	4	4	?						✔
	EN	3	3	?						?
	EN	3	3	✔						✔
	EN	4	4	✔						✔
	EN	4	4	✔						✔
Candidates from name collision studies										
	—	4	4	?						✘
	—	5	5	✘						✘
	EN	4	4	?						✘
	—	3	3	✘						✘
	EN	11	11	✔						✘
	EN	4	4	✘						✘
	EN	9	9	✘						✘

.INTERNAL has been selected

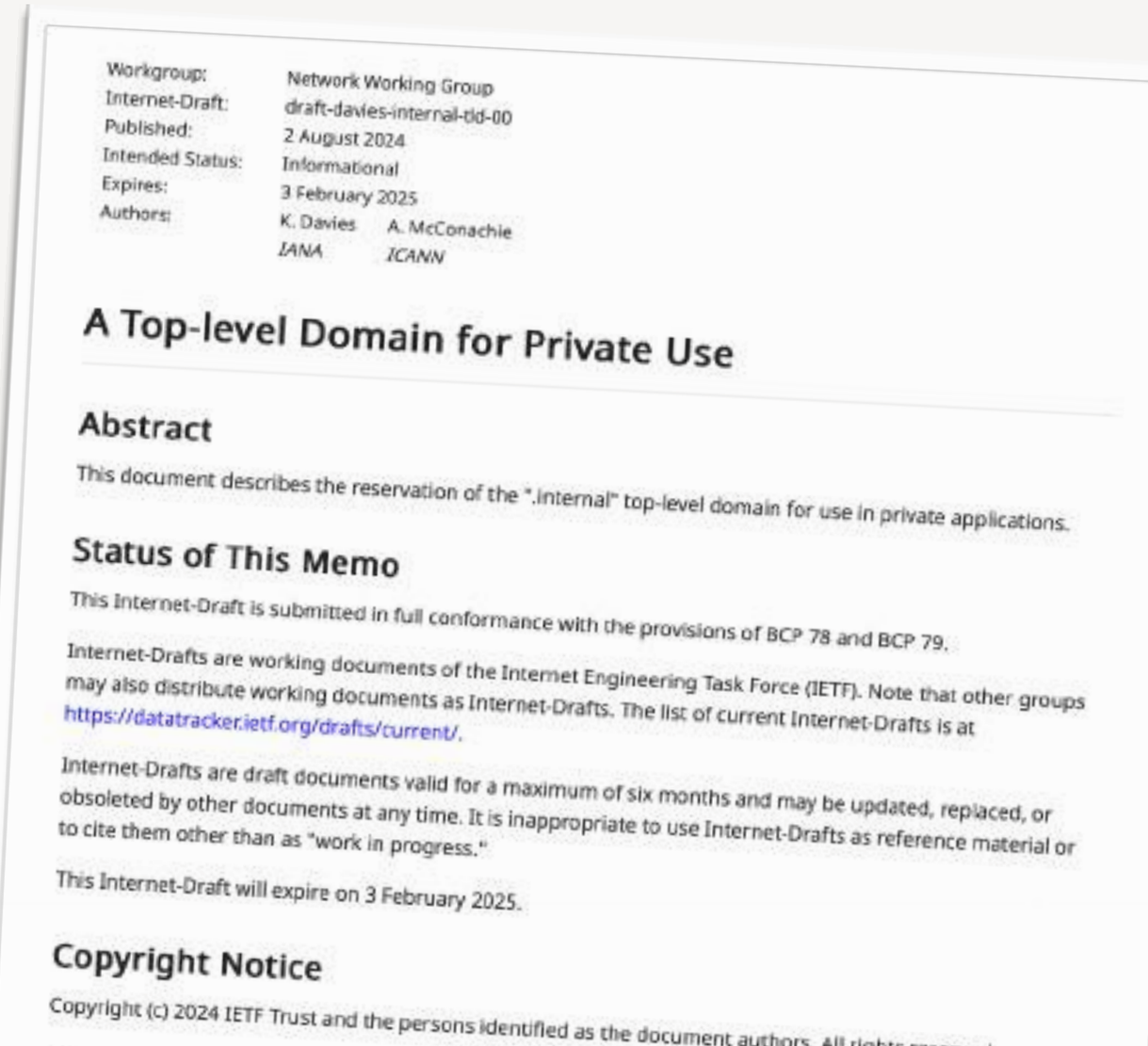
- IANA determined the .INTERNAL was the superior choice based on its assessment.
- Put for public comment
  - Various opinions sought additional reservations, or a different reservation based on preference or on criteria that were not specified in SAC113.
  - No feedback suggested the analysis didn’t fulfill SAC113 criteria
- ICANN Board adopted the recommendation and permanently reserved .INTERNAL for private-use purposes.

.INTERNAL vs existing alternatives

- There are other reserved namespaces that look the same but serve different purposes
- .LOCAL (RFC 6762)
  - Multicast DNS protocol
- .ALT (RFC 9476)
  - For DNS-like namespaces that are not the DNS
- HOME.ARPA (RFC 8375)
  - Home network autoconfiguration using certain protocols
  - Special handling — never leaves local network.
  - Replaces “.HOME” that was unofficially used (i.e. RFC 7788)
- .INTERNAL supports no specific protocol and has no special resolution logic

Documenting .INTERNAL

- Working on an Internet Draft: draft-davies-internal-tld
- Will produce explanatory IANA material (help documents, etc.)
- Next-generation Root Zone Database on IANA website will include reserved names (and as a result, in WHOIS/RDAP too.)



Workgroup: Network Working Group
Internet-Draft: draft-davies-internal-tld-00
Published: 2 August 2024
Intended Status: Informational
Expires: 3 February 2025
Authors: K. Davies, IANA; A. McConachie, ICANN

A Top-level Domain for Private Use

Abstract

This document describes the reservation of the ".internal" top-level domain for use in private applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 February 2025.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights

Next round of new gTLDs

The next round of new gTLDs

- ICANN has conducted three rounds of expansion of generic top-level domains to date
  - Before any rounds — created before ICANN
    - .com, .edu, .gov, .int, .mil, .net, .org
  - 1st round — “Proof-of-concept” round (2000)
    - .aero, .biz, .coop, .info, .museum, .name, .pro
  - 2nd round — “Sponsored” round (2003)
    - Limited to namespaces with novel purposes and closed communities
    - .asia, .cat, .jobs, .mobi, .tel, .travel, .xxx
  - 3rd round — “New gTLD Program” (2012)
    - Significant expansion adding over 1,000 new TLDs
- ICANN is now embarking on its fourth application round
  - 4th round — “New gTLD Program: Next Round” (2026)
    - Refined process similar to the 3rd round

IANA's role

- IANA's role essentially begins "post-contracting"
  - Converting an eligible operator of a new gTLD, with contract signed, into a working gTLD
  - There is a handoff from the application system to IANA to conclude the gTLD's establishment
  - IANA's process involves
    - Independently validating policy criteria are met
    - Establishing IANA-specific details
    - Creating the TLD in the root zone
  - Each new TLD becomes an enduring IANA customers we need to support
- In the previous round, IANA was also responsible for limiting rate of change for root zone
  - Previously limited to 1,000/yr (translated to 20/wk)
  - Now a percentage rate of change of 5%/month
    - Be mindful of compounding effect

Name Collision

- Name Collision generally refers to the unapproved use of domain names conflicting with official uses, such as when TLDs are delegated for the first time
  - In particular, poses security risks where traffic originally never materializing on the global Internet can suddenly be redirected to a new location.
- Earlier this month, ICANN Board “approves all the recommendations in the NCAP Study 2 Final Report, with the sole exception of Recommendation 4.1”
  - “Recommendation 5 - ICANN must support the delegation of strings in order to improve the ability to conduct a name collision risk assessment”
  - A new function, the Technical Review Team, will be established to receive data based on such technical delegations, prior to the legal delegation of a new gTLD.
  - This team will make findings on high-risk domains that post a risk in name collision

Name Collision

- IANA will need to model this into its business processes
  - Temporarily delegation for TRT assessment wouldn’t constitute a legal delegation to a new party
  - More akin to the temporary delegation of test TLDs that happened in the mid-2000s to prove out IDN support
    - These domains had no registry operator or other characteristics of a production TLD, largely involved NS records and nothing more.
  - Need to work on various elements on how these will work
    - Integration with ICANN systems to trigger the addition and removal in the root zone
    - Adhering to root zone change limits
    - How to appropriately reflect the status of these labels (e.g. Root Zone Database, WHOIS, RDAP, machine readable formats)

Variants

- Variants refers to the handling of confusable alternate labels in IDN registrations
- Variants are not currently an official consideration in root zone management policy
  - However, some delegations, while not considered variants, functionally operate as variants e.g. Traditional and Simplified Chinese labels.
- Both the next round and emerging ccNSO policies envisage a formalized approach to variants
- Proper variant support has a profound impact on administration
  - Conceptually moves business operations from mapping domains to labels from 1-to-1 to 1-to-many.
  - Special business rules around retaining the integrity of the set and managing conflicts
  - Operationally treating multiple labels and a holistic set and only exposing the variants in technical contexts where needed.
- IANA has done preliminary work (repository, RFC 7940), but significant work to come.

Machine Readable Registries

Work on Machine Readable Registries

- Most IANA data is published in machine readable form
  - 3,000+ protocol parameter registries
    - XML is the normative version
    - HTML, TXT, CSV derivatives
  - Some specialized registries have different formats
    - MIB files, YANG modules, language subtags, etc.
- What we're working on
  - Creating JSON as a new consumable format for all registries
  - Implementing machine readable formats for Root Zone Database
    - Decide what data should be machine readable
    - Testing against common use cases that IANA is often asked to provide
    - In concert with other activities, including adding reserved domains, historical entries, new visual presentation (likely based on same JSON).

Thank you!

kim.davies@iana.org