Evolving Root Zone Authentication

ICANN DNS Symposium
November 2022

Kim Davies
VP, IANA Services, ICANN
President, PTI

PTI | An ICANN Affiliate
Introduction

• The root zone trust model has been essentially unchanged for decades
• The current model doesn’t adapt well to all modern usage requirements
• We are taking our first steps toward evolving:
  • Separating public POC from authorization responsibilities
  • Providing granular rights for individual users
• Work to be done (and discussed today):
  • Improving authentication practices
Next-gen focus areas

**New authorization model.** Separation between public points of contact and users who can submit and authorize requests.

- **Administrative Contact**
  - Listed in public WHOIS
  - Approves change requests
  - Must be in country (ccTLDs)

- **Technical Contact**
  - Listed in public WHOIS
  - Approves change requests

- **Authorising Contacts**
  - Not published (managed via RZMS)
  - Approves change requests

**New Flexible Model**

- One or more (no fixed number)
- Must be persons (no role accounts)
- Stronger identity controls
- Flexible threshold approval options
- In-country requirements?

---

**Transition process**
Next-gen focus areas

Approval thresholds. Decide how many contacts must approve changes (1, 2, 3 or more, or all.)

Granularity. Authorizers can be configured to be (technical, not-technical, transfers etc.)


Automation. Development of APIs and other tools to help automate and manage large portfolios.
Today

- Each TLD has two points of contact
  - Administrative and Technical Contact
- Both must **cross-authorize** all types of changes to a TLD in the root zone
  - Exception for ccTLD transfers - requires separate instrument
- Increasingly, many operators have moved to role accounts to hide any internal complexity associated with process general enquiries, approvals and the like
  - Net result: Lack of transparency, hard for IANA to understand and diagnose
  - Lack of identity makes enhanced authentication controls difficult
ICANN “SSR2” Study

- ICANN org and PTI operations **should accelerate** the implementation of new Root Zone Management System (RZMS) **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. (Recommendation 21.1)
Root Zone Update Study

- We do not recommend implementation of a traditional multifactor authentication system for the RZM currently.

- The operators that perceive the need for multifactor authentication are not considering the multiple layers of protection and the de-facto multifactor requirements for access to the Registry’s zone file and to an employee’s email account. We suggest IANA continue communications with TLD managers to gain a common understanding of the multiple levels of authentication and authorization in use as the process is executed.

- We recommend refinement of RZM interactions to eliminate the potential for data leakage that could facilitate social engineering-type attacks, including but not limited to: eliminating sensitive content in emails, the use of persistent authentication in HTTPS links, and the availability of ticket information in unauthenticated sessions.
Our take

• We have conflicting advice on what to do
• Some subset of TLD operators clearly want multi-factor authentication
• Expect to introduce an implementation that is opt-in
• We’ve started on a path to evolving forward
  • First step, independent user accounts for individuals
• But we have a lot of challenges to consider
  • Account recovery is key
Technological considerations
Worldwide availability

- The IANA services are provided to every country in the world
  - ... including in locations that may be otherwise prohibited
- IANA needs to be able to successfully deliver services to all its customers
  - We cannot implement required mechanisms that only work in limited locations
- Also limits our ability to leverage third parties — which IANA may be permitted to work with certain entities, our suppliers may not
  - We are also incentivized to limit third parties as we may not be able to rely upon them in an emergency
Telephone based authentication

- We believe phone based authentication should be avoided
  - Customer is not in full control of their phone service, and can be subject to SIM hijacking attacks and the like
  - Cannot guarantee reliable delivery across all of our service areas
    - e.g. Mandatory code recital from an SMS sent in-flight
  - Could serve as a form of additional verification, or notification of account activity, but should never be a primary method (or only method!) of authentication
Which leads us to..

- Time-based one-time passwords (TOTP)
- Web Authentication standard (WebAuthn)
Time-based one-time password (TOTP)

- TOTP is a well-adopted and simple to implement
  - Simple algorithm generates a code that changes every 30 seconds
  - Induction through a shared secret sent from server to client (often via QR code)
  - Code is a hash of the shared secret and the time
  - Server can define a expandable window of acceptable responses to account for time drift, typing delays
  - Many free implementations, and built into recent operating systems directly
- It is an unencumbered IETF standard (RFC 6238)
- Most users will have familiarity with this, and have the tooling to use it
WebAuthn

- Web Authentication (WebAuthn/FIDO2) is a W3C standard for authentication with private keys
- This year major vendors have announced significant support for it as the primary/only factor.
  - Passkeys in iOS/macOS/Android/Chrome/etc.
  - Private keys retained on device, protected by inherent security mechanism (e.g. “secure enclave”/HSM) typically unlocked by biometrics
- While use as the sole factor is not multifactor authentication, it realizes similar security benefits and could be considered an alternative to the username/password/factor paradigm
- Requires education and discipline with customers to ensure they enroll multiple redundant devices, or there are suitable fallback options
  - Unlike multifactor token, which often sync between devices, tokens are not transferrable and you generate unique keys for each device
Illustrative workflows

Conventional login

Step 1
Provide username and password

Username
Password
Login
Illustrative workflows

TOTP as 2nd factor

Step 1
Provide username and password

Username

Password

Login

Step 2
Provide token

Provide 6-digit code from your authentication app

Login
Illustrative workflows

WebAuthn as 2nd factor

Step 1
Provide username and password

- Username
- Password

Step 2
Respond to cryptographic challenge

Approve login using your biometric ID or authenticator device
Illustrative workflows

WebAuthn as primary factor

Step 1
Respond to cryptographic challenge (identity is derived from the account the private key is associated with)

Approve login using your biometric ID or authenticator device
Operational considerations
Operational choices

• Fundamentally, we see this as an operational challenge
  • TOTP is extremely simple to implement, WebAuthn is achievable
  • Well established protocols on how they should operate based on common adoption across the industry
• However, our usage model differs from convention
• Problems exist outside the “ideal” workflow where the customer has all their credentials available
Our biggest concern

- Most customers rarely use our service
  - Many will go many years between interacting with IANA
  - When they do, today we see a reasonable likelihood they have lost their credentials and will need to conduct a username/password reset
  - MFA will not solve this, it will make it worse
  - A proper implementation cannot allow an MFA reset, therefore new robust procedures must be implemented
- We know very little about our customers today to effectively conduct such resets
  - Personal relationships with most contacts is no longer possible
- When customers do need to make changes, they are sometimes urgent in nature
Emergency Availability

- We need options of restoring trust in a compromised network connectivity situation
  - Restoration of TLD service, may be cause by a widespread outage such as natural disaster
- Email contacts are particularly vulnerable in such a situation, so are not a good presumptive fallback option.
  - Many email accounts in in-bailiwick of the associated TLD
  - No custom of ensuring alternatives that are outside of the impact scope
Knowing our customers

- To reset credentials, we need to reliably satisfy that we are interacting with the correct party
- Instituting more comprehensive “know your customer” (KYC) protocols would seek to add the capability to reliably do this
  - Comes with associated risk through increased PII collection
- Can we use vendors for the normal case?
  - Third-party services to perform identity validation without passing specifics to IANA, vouches to IANA formal legal name and limited set of particulars
- Is it appropriate for users to opt-out, effectively giving IANA no pathway to restore trust if it cannot establish their identity?
  - When there is a TLD emergency, it is imperative to restore operation
Staff turnover

- Given the long time between IANA interactions, staffing can change at the associated organizations.
- While moving from role accounts to a person-based user model will realize benefits, it will incur a greater need to track to those staffing changes by adding/removing users over time.
- We expect we are going to need to get greater understand through experience on how to optimize these workflows.
Ensuring authentication remains usable

- Preventative measures could reduce the surprise when a customer seeks to interact and finds they don’t have accurate credentials.
- Periodic reminders to check accuracy of records
  - e.g. a quarterly reminder of the details we have on file, presenting an opportunity to correct or update
- Some form of “forced” authentication could be a component
  - Active check-in to verify authentication methods work etc.
  - A lack of successful login after a period marks the account dormant, triggers other corrective action
- What are reasonable requirements that IANA can ‘require’ to advance in these areas?
Next steps
Next steps

• We are in the early phases of thinking about how we’d want to implement increased authentication options
• Looking for feedback and expertise that inform our thinking
• We’d like to assess the appetite for elevating the baseline requirements in this area
• TLDs are critical infrastructure