ICANN | GAC
Governmental Advisory Committee

85 | COMMUNITY FORUM

DNS for Digital Identity: Evolving a Trusted Internet Protocol

(Proposed by the India GAC Delegation)

Session 18 - Emerging Topics for GAC Discussion

Session Objective

This GAC Plenary Session is proposed by the host country GAC Delegation, under the umbrella of GAC Strategic Objective #7 Impact of New Technology on Internet Unique Identifier Systems: "*The GAC will increase understanding and raise awareness of the challenges and opportunities of new technologies as they relate to the Internet's unique identifier systems. To that end, the GAC will leverage the expertise in the ICANN Community, governments and beyond, to share information and consider potential implications, for the benefit of GAC members and all stakeholders".*

The proposed session is expected to align with several of the Expected Outcomes for this Strategic Objectives in the GAC Annual Plan 2025/2026 including those related to Artificial Intelligence (7.2) Blockchains (7.4) and Cryptography (7.5). It also relates to DNS Abuse Mitigation (GAC Strategic Objective 4 and related Expected Outcomes).

For more than four decades, the Domain Name System (DNS) has served as one of the Internet's most trusted and resilient protocols, providing a globally interoperable framework for naming and resolution. While DNS was not designed as an identity system, its structure, cryptographic extensions, and operational maturity have increasingly positioned it as a foundational layer for digital trust. At the same time, emerging decentralized technologies are expanding the role of names, linking them to authentication, digital assets, and cross-platform identifiers, often outside established governance and security models.

This session examines how DNS can evolve, without disruption, to function as a foundation for digital identity through a Universal Resolution approach that remains fully compatible with the existing DNS hierarchy by leveraging the DNS resolver logic. It explores how decentralized components such as distributed zone storage, blockchain based namespaces, machine-learning–driven abuse detection, and privacy-preserving cryptographic techniques (including zero knowledge proofs) can be integrated in a controlled, standards-aligned manner.

The discussion will address practical considerations around security, accountability, and compliance requirements, including DNS Abuse Mitigation, offering a pragmatic blueprint for extending Internet naming while preserving the trust, stability, and global interoperability.

Session Information

Session Duration:

45 minutes, as part of the shared session on Emerging Topics for GAC Discussion

Session Agenda:

Presentation (30 min) - *Slides are provided in Annex to this briefing*

1. Universal Resolver: bringing decentralized namespaces into the mainstream and resolvable by traditional DNS services
2. Creating value-addition through blockchain and Non Fungible Tokens (NFT)
3. AI for DNS Abuse mitigation: random forest (classification tree) model to identify DNS Abuse threats

Q&A (15 min) Which is expected to include governance considerations (risks, challenges and opportunities)

Presenter:

Dr. Balaji Rajendran,
Scientist F & Group Head, at the Centre for Development of Advanced Computing, Bangalore.

Key Reference

- B. Rajendran, G. Palaniappan, D. R, B. B. S and S. S D, "A Universal Domain Name Resolution Service – Need and Challenges - Study on Blockchain Based Naming Services" 2022 IEEE Region 10 Symposium (TENSYMP), Mumbai, India, 2022, pp. 1-6, doi: 10.1109/TENSYMP54529.2022.9864361.
- The presentation material for this session are included as Annex to this briefing

Further Information

GAC Participants may wish to refer to the ICANN78 Hamburg GAC Capacity Development Workshop which included several sessions discussing blockchain technology, blockchain-based alternative namespaces and associated policy issues. The recording and material of these sessions is available on the GAC website and is linked below.

- **Introduction to the Namespace and Case Study**
  (GAC Capacity Development Workshop Session 6) - Transcript | Recording
  - Presentation: Challenges with Alternative Name Systems by Alain Durand, Distinguished Technologist, ICANN OCTO
  - Document: Challenges with Alternative Name Systems, ICANN Office of the Chief Technology Officer (27 April 2022)

- **Blockchain - Introduction and Applied Learning**
  (GAC Capacity Development Workshop Session 7) - Transcript | Recording
  - Presentation: How blockchains name systems works by Paul Hoffman, ICANN OCTO
  - Presentation: Blockchains in 12 Easy Steps by Alain Durand, Distinguished Technologist, ICANN OCTO

- **Alternative Namespaces: Policy Issues for the GAC**
  (GAC Capacity Development Workshop Session 8) - Transcript | Recording
  - Speakers:
    - DNS Research Federation – Georgia Osborn
    - Greenberg Traurig LLP – Marc Trachtenberg
    - Porkbun - Ray King
    - Verisign – Swapneel Sheth
    - Afnic (registry for .fr) – Régis Massé
    - WIPO - Brian Beckham

- **Breakout Sessions - Alternative Name Space and Emerging Technology Challenges: Identifying Government Technology Policy Interests and Concerns**
  (GAC Capacity Development Workshop Session 9 and 10) - Part 1 Transcript | Recording and Part 2 Transcript | Recording
  - Presentation: Discussion Questions for GAC Participants

Document Administration

Title	ICANN85 GAC Session Briefing - Emerging Topics for GAC Discussion: DNS for Digital Identity
Distribution	GAC Members (before meeting) and Public (after meeting)
Distribution Date	Version 1: 17 February 2026

DNS for Digital Identity: Evolving a Trusted Internet Protocol

Dr. Balaji Rajendran
Scientist F
Centre for Development of Advanced Computing (C-DAC)
Ministry of Electronics and Information Technology (MeitY)
Government of India

DNS: A Foundational Element for Trust

Globally Unique Namespace

Maintains distinct domain names, preventing conflicts and supporting global addressing

Hierarchical Delegation

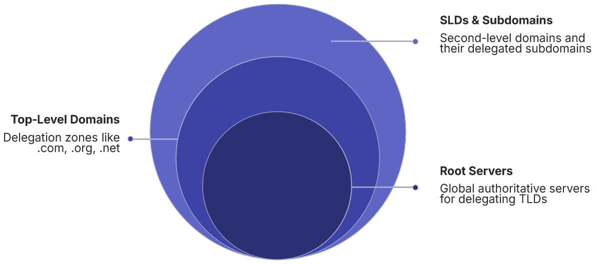
A structured approach enabling distributed management

Operational Resilience

Anycast routing, redundancy, and diverse infrastructure, supporting service availability.

DNSSEC Chain of Trust

Cryptographic security for DNS ensuring the authenticity of DNS data.



SLDs & Subdomains
Second-level domains and their delegated subdomains

Top-Level Domains
Delegation zones like .com, .org, .net

Root Servers
Global authoritative servers for delegating TLDs

The Expanding Role of Names

Domain names have developed beyond their initial function of resolving IP addresses. They now serve as identifiers and trust mechanisms within an expanding range of digital applications.

01

Address Mapping

The foundational role of DNS, translating human-readable domain names into IP addresses for network routing.

02

Authentication Anchor

Evolution with DNSSEC, serving as a critical infrastructure component for cryptographically validating domain origins and enhancing security.

03

Brand Trust Signal

Domain names as indicators of legitimacy and credibility, contributing to online business operations and consumer confidence.

04

Digital Asset Linkage

Integration with distributed ledger technologies for associating decentralized identifiers, digital wallets, and related assets with human-readable names.

05

AI/API Agent Identity

The role of DNS in providing verifiable identities for automated systems, APIs, and AI agents within machine-to-machine interactions is under exploration.

The Case for a Universal Name Resolution Service

A Universal Name Resolution Service addresses the critical infrastructure challenge of namespace fragmentation, providing unified resolution across traditional and emerging identity systems while maintaining security and governance standards.

The Need: Breaking the Silos

- Prevents the fragmentation of the Internet by providing a unified resolution layer across disparate namespace systems.
- Without universal resolution, each namespace operates in isolation, creating security gaps, user confusion, and governance challenges that undermine the stability of digital identity infrastructure.

The Importance: Integrated AI Defense

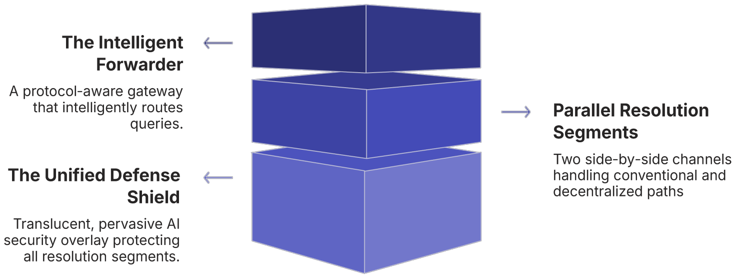
- As namespaces proliferate, the probability of malicious domains increases exponentially.
- A universal resolver enables **cross-system threat intelligence, behavioral analysis, and coordinated security responses** creating a unified watchdog that detects attack patterns invisible to isolated namespace systems.

The Benefit: Seamless Access

- One-time configuration enables users to navigate effortlessly between classical and decentralized namespaces without understanding underlying protocol differences.
- This eliminates friction, reduces user error, and democratizes access to emerging digital identity systems.

The Universal Name Resolution Service (UNRS): A Modular Orchestration Framework

UNRS provides a modular, protocol-aware resolution architecture that unifies traditional and decentralized namespace systems while maintaining security, and governance standards through intelligent routing and cross-namespace threat detection.



The Intelligent Forwarder

A protocol-aware gateway that intelligently routes queries.

The Unified Defense Shield

Translucent, pervasive AI security overlay protecting all resolution segments.

Parallel Resolution Segments

Two side-by-side channels handling conventional and decentralized paths

By centralizing resolution logic, we eliminate identity fragmentation while preserving the authoritative root.

Building Upon Existing Standards

This proposes to leverage established RFCs and standards, and at the same time resolve Decentralized Digital Identifiers.

1

RFC 1034 / 1035

Defines the fundamental architecture and protocols for the Domain Name System, establishing the hierarchical naming structure and resolution mechanisms that underpin the internet.

2

DNSSEC (RFC 4033–4035)

Introduces cryptographic security to the DNS, providing authentication of DNS data origin and integrity protection against various attacks like cache poisoning.

3

RFC 8806 (Hyperlocal Root)

Proposes methods for operating a root name server instance close to a DNS resolver, enhancing privacy, resilience, and performance for local resolution.

4

RFC 6698 (DANE)

Specifies a protocol for binding X.509 certificates to DNS names using DNSSEC, enabling secure distribution of cryptographic keys and enhanced service authentication.

5

Emerging DNS-based DID

Explores the integration of Decentralized Identifiers (DIDs) with the DNS, leveraging existing infrastructure for discovery and resolution of self-sovereign digital identities.

AI in the DNS Ecosystem

DGA Detection

Identifying Domain Generation Algorithm patterns used by malware to generate domain names for command-and-control servers.

Fast-Flux Analysis

Detecting rapidly changing DNS records and IP addresses associated with malicious infrastructure to evade detection.

Phishing Detection

Recognizing suspicious domain patterns, typosquatting attempts, and other indicators of phishing campaigns.

Abuse Mitigation

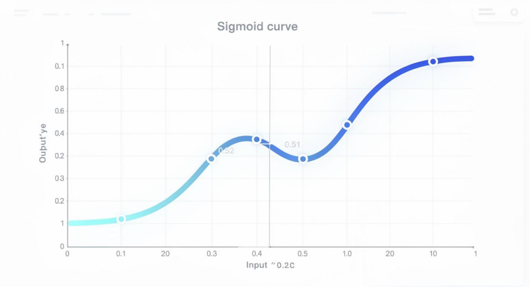
Automating responses to DNS-based threats and policy violations, enabling more timely and extensive protective actions.

These developments are being discussed within the IETF, particularly by the AINetOps working group and in various DNSOP drafts concerning AI agent naming. This reflects ongoing efforts to integrate AI within established internet standards and governance frameworks.

Mathematical Foundations

AI models deployed in DNS security utilize relevant mathematical functions to convert raw model outputs into probabilities for threat detection and mitigation efforts.

The Sigmoid Function: Converting Outputs to Probabilities



Maps Raw Model Output to 0–1 Probability

The Sigmoid function accepts any real number as input and transforms it into a value strictly between 0 and 1. This conversion allows the model's output to be interpreted as a probability score, supporting structured analysis.

For instance, a value of 0.95 indicates a 95% probability of a specific event (e.g., a domain being identified as malicious), providing interpretable risk scores from model outputs.

Supports Risk Scoring Thresholds

The Sigmoid function assists in setting defined thresholds for automated responses, in accordance with established policies.

For example, a probability score exceeding 0.8 could initiate an alert for high-risk activity, while a score above 0.9 might automatically initiate a block on a domain based on pre-defined operational rules.

Brief on Model Training

These AI models are trained by minimizing **loss functions** (such as cross-entropy), employing optimization algorithms like **gradient descent**.

This iterative process adjusts the model's parameters to converge to an optimal state, progressively enhancing the accuracy and reliability of its predictions within defined operational parameters.

The Calculus of Defense: Optimizing the Shield

$$S(z) = \frac{1}{1 + e^{-z}}$$

Sigmoid Mapping

The Sigmoid function, as shown above, maps raw network signals to a 0-1 probability range. This provides a "**Reputation Score**" rather than a binary block decision, enabling granular threat assessment.

Loss Minimization

Binary Cross-Entropy is employed to train the model, a critical method for optimizing **model accuracy** in threat classification by penalizing incorrect predictions.

The Optimum

Gradient Descent is iteratively applied to reach the global minimum of error, ensuring the **continuous improvement** of model performance and convergence towards optimal parameters.

Why Random Forest (RF)?

Random Forest seeks the global maxima of Information Gain in decision trees. This ensures features such as `lexical entropy` (for DGA detection) are weighted correctly against `temporal history`, leading to balanced feature importance for comprehensive threat assessment.

AI for DNS Abuse Mitigation

- AI models contribute to DNS security by employing a feature-based risk scoring approach.
- This facilitates the identification and mitigation of various forms of DNS abuse by providing data-driven insights.

Key Features Analyzed for Risk Scoring

Lexical Entropy

Analyzes the randomness in domain name characters, an indicator for detecting Domain Generation Algorithms (DGAs) often used in malware.

TTL Volatility

Monitors anomalous changes in Time-To-Live (TTL) values, which may indicate attempts to evade detection or manipulate DNS resolution.

Registration Age Anomalies

Identifies newly registered domains or those with unusual historical registration patterns associated with malicious campaigns.

IP Reputation

Assesses the historical behavior and known threat intelligence associated with the IP addresses linked to a domain, to assess potential risk.

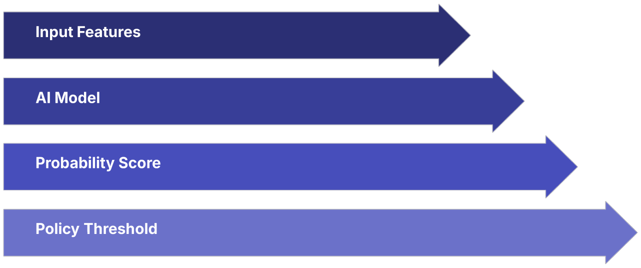
Behavioral Deviations

Detects anomalous changes in query patterns, traffic volumes, or other behavioral metrics that may suggest a new threat.

AI as a Supporting Tool for Governance

Decision Flow: AI-Powered Risk Assessment

- Diverse input features are processed by the AI model to yield a probability score
- This is evaluated against predefined policy thresholds for a decision.



Emerging Trends: AI & DNS in IETF Discussions

- The intersection of Artificial Intelligence (AI) and the Domain Name System (DNS) is an area of ongoing standardization efforts within the Internet Engineering Task Force (IETF).
- Numerous drafts and working groups are dedicated to examining the challenges and considerations presented by this convergence.

1

DNS-Native AI Agent Naming Draft

A proposal to standardize methods for identifying and resolving AI agents directly through the DNS infrastructure, facilitating integration.

2

DNSOP Draft on DNS for Internet of Agents

Discussions within the DNS Operations (DNSOP) Working Group focusing on the implications of agent-to-agent communication and naming conventions for the DNS.

3

AINetOps Operational AI Draft

The AI for Network Operations (AINetOps) Working Group is exploring practical applications of AI to enhance the operational efficiency and resilience of network infrastructure.

Digital Asset Transformation: A Value Proposition for DNS

The conversion of classical domain ownership into Non-Fungible Tokens represents a fundamental shift toward immutable data and verifiable digital identity.

From Classical to Tokenized Assets

- **NFT tokenization** transforms domains into **verifiable digital assets** with cryptographically secured ownership records.
- The blockchain-based approach ensures that every transaction, transfer, and modification is permanently recorded, creating an unalterable chain of custody that establishes provenance and authenticity.

Day Zero Audit Trail

- Recording ownership and behavior from Day Zero enables mathematical tracking of domain reputation.
- Historical data such as ownership transfers becomes quantifiable, allowing algorithmic assessment of trustworthiness.
- This creates a **reputation economy** where domain value is directly tied to verifiable behavior.

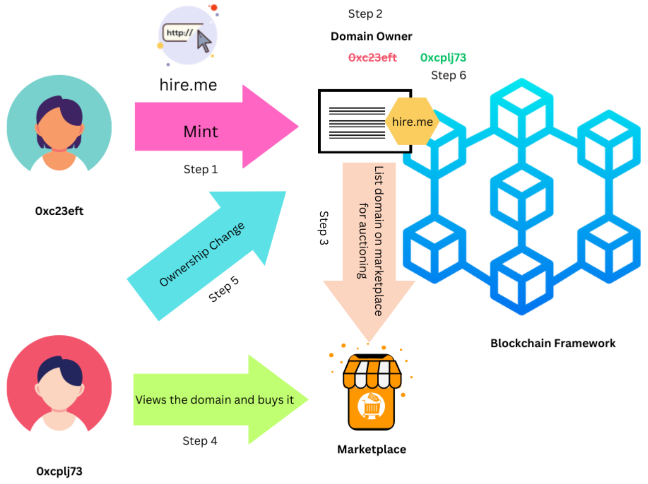
Case Study: Tracking malicious or scam domains through permanent ledger records prevents re-registration and enables proactive threat identification across the namespace.

Reputation-Based Leasing

- **Domain-as-a-Service** (DaaS) enables high-reputation domains to function as Verified Digital Identities available for short-term leasing.
- Organizations can leverage established trust without permanent acquisition, while domain owners can monetize reputation capital.

Technical Anchor: NFTs incorporate legally valid digital signatures within smart contracts, establishing cryptographic proof of authenticity and enhancing credibility in secondary markets.

Classical Domains as NFT



The NFT Identity for DNS - Example

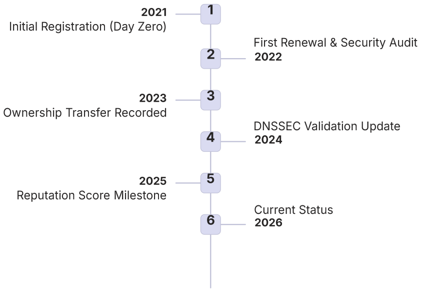
Digital Identity Instrument

1

abc.xyz
Registered: 2021
Reputation Score: 98/100
Verified via DNSSEC
Owner: [Organization Name]
Status: Active

The Day Zero Reputation Anchor

Immutable Lifecycle Ledger



1 **2021** Initial Registration (Day Zero)

2 First Renewal & Security Audit **2022**

3 **2023** Ownership Transfer Recorded

4 DNSSEC Validation Update **2024**

5 **2025** Reputation Score Milestone

6 Current Status **2026**

Functional Architecture:

- Tokenization creates an unalterable history, ensuring that reputation cannot be erased or faked
- Every event is cryptographically recorded on the blockchain, providing non-repudiable evidence
- The NFT serves as an identity instrument that carries verifiable reputation

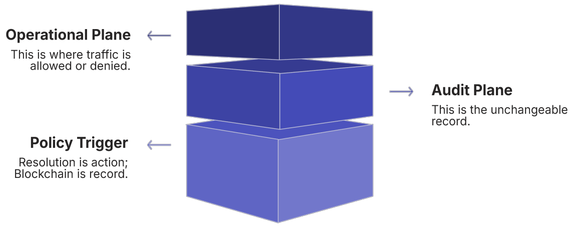
Technical Benefits:

- Day Zero recording establishes complete provenance
- Reputation scoring becomes mathematically verifiable
- Dispute resolution (UDRP) can gain access to complete audit trail
- Secondary market transactions include full transparency

Tokenize the domain to create an unalterable history, ensuring that reputation cannot be erased or faked.

Bridging Accountability: Compliance in a Layered Architecture

The system **separates resolution policy from audit history**, enabling regulatory compliance without sacrificing accountability.



Operational Plane
This is where traffic is allowed or denied.

Audit Plane
This is the unchangeable record.

Policy Trigger
Resolution is action; Blockchain is record.

Technical Architecture

- **Blockchain provides the Witness (Audit); The DNS Resolver provides the Enforcement (Resolution)**
- Resolution suspension does not erase the audit trail, ensuring both legal compliance and forensic integrity
- This architectural separation enables protocol stability, regulatory compliance, and enhanced accountability within a unified framework

This architecture ensures that legal compliance (Takedowns) does not compromise the forensic chain of custody (Accountability).

What This Does NOT Do

This section clarifies the scope of this proposal, specifically outlining what it does not entail, to address potential concerns. This initiative is intended to complement existing internet infrastructure and governance, rather than disrupt it.

Does not establish an alternative root

- The ICANN root remains the authoritative source for the Domain Name System.
- No competing or parallel root systems are introduced through this proposal.

Does not circumvent ICANN governance

- All proposed modifications adhere to and operate within established ICANN multistakeholder processes.
- Existing governance structures remain preserved and authoritative.

Does not supersede PKI

- Public Key Infrastructure and Certificate Authorities continue to operate as foundational elements.
- This complements, rather than replaces, established trust mechanisms.

Does not mandate Blockchain integration

- Blockchain integration is **an optional component**, not a mandatory requirement.
- Traditional DNS operations maintain their existing functionality without modification.

Does not cause namespace fragmentation

- The unified, globally consistent DNS namespace is maintained.
- This approach avoids the introduction of namespace collisions or conflicting identifier systems.

Proposed Outcomes

The DNS is undergoing an evolution to address requirements for digital identity, ensuring secure interactions and maintaining its foundational principles of stability and interoperability within established frameworks.

1

Resolution Mechanisms

2

Trust Frameworks

3

Identity Coordination

1. Source of Trust

- The ICANN root acts as authoritative source.
- Avoidance of fragmentation or competing systems is maintained.

2. Adherence to multistakeholder governance

- Existing governance models are preserved and reinforced.
- Community-driven decision-making processes continue.

3. Sustained global interoperability

- Functional operation across traditional and evolving systems is ensured.
- Broad compatibility and accessibility are maintained.

4. Guided evolution

- A measured, standards-based approach informs development.
- Existing infrastructure is respected while accommodating future capabilities.

Thank You

I Welcome Your Questions and Perspectives I

Dr. Balaji Rajendran | C-DAC Bangalore, MeitY