

Enhancing Justifiable Trust in the use of the Internet and Email

Hosted by the National Internet Exchange of India (NIXI)

Report by Maarten Botterman and Sameer Gahlot

A Shared Challenge: Trust in the Digital Age

On 8 March 2026, during ICANN85 in Mumbai, the Global Forum on Cyber Expertise (GFCE) convened a Triple-I capacity-building workshop focused on a question that is becoming increasingly urgent:

How can we increase justifiable trust in the use of the Internet and e-mail, world-wide?

The workshop brought together policymakers, technical experts, industry leaders, and members of the global Internet community. While participants represented different sectors and regions, they shared a common recognition: the Internet has become indispensable infrastructure, yet trust in its use is under pressure.

The rapid growth of digital services, particularly in countries like India, now home to more than a billion Internet users, has created unprecedented opportunities. At the same time, it has exposed users and institutions to rising levels of fraud, impersonation, and manipulation. Technologies such as artificial intelligence, while powerful, further amplify both opportunity and risk.

The message that framed the day was clear:

Connectivity alone is no longer enough. Trust must be built into the Internet itself.

The GFCE Triple-I initiative, launched to address precisely this challenge, focuses on strengthening Internet infrastructure through awareness, adoption of open standards, and multistakeholder collaboration. The Mumbai workshop marked an important milestone as the first Triple-I session held alongside a global ICANN meeting, reinforcing the link between technical expertise and policy development.

1. Setting the Stage: Why Trust Must Be Engineered

The workshop opened with strong recognition of the importance and urgency of increasing trust in digital systems at a time we are increasingly dependent on those, and “the bad guys” increasingly exploit the remaining vulnerabilities.

In a recorded message, Vint Cerf, one of the founding architects of the Internet, reflected on the broader erosion of trust in the digital environment. He highlighted how emerging technologies, particularly artificial intelligence, are making it increasingly difficult to distinguish authentic from manipulated content, and stressed the importance of verifiable systems. He framed the challenge succinctly:

“We are entering a world where we must be able to verify not just what we receive, but who—and what—is behind it. Trust in the Internet will depend on our ability to build systems that are accountable, auditable, and worthy of that trust.”

This message set a powerful context for the workshop, linking infrastructure-level security directly to broader societal trust.

From a national perspective, Sushil Pal, Joint Secretary at the Ministry of Electronics and Information Technology (MeitY), India, provided a grounded and highly relevant framing of the challenge. He emphasized that India’s rapid digital transformation—now encompassing more than one billion Internet users—has created both opportunity and exposure.

He noted that many users are relatively new to digital services and therefore particularly vulnerable to sophisticated forms of cybercrime, including phishing, impersonation, and emerging social engineering techniques such as so-called “digital arrest” scams.

In this context, he stressed that trust cannot be addressed at a single layer:

“As our digital ecosystem grows, trust must be built across every layer—from infrastructure to applications to user awareness. Security cannot be an afterthought; it must be embedded by design.”

He further underlined that initiatives such as trusted domain spaces and strengthened infrastructure standards are essential to protecting citizens and enabling confidence in digital services.

From the global policy perspective, Nico Caballero, Chair of the ICANN Governmental Advisory Committee (GAC), reinforced that Internet infrastructure has evolved into a cornerstone of national and global economies. As such, its resilience and trustworthiness are no longer purely technical concerns, but central policy priorities.

He emphasized that governments increasingly depend on the Internet to deliver essential services and support economic development, and that this dependency requires a corresponding commitment to securing the underlying infrastructure.

In his intervention, he highlighted the importance of open standards and multistakeholder cooperation:

“The strength of the Internet lies in its open, interoperable architecture. Ensuring its security and resilience requires collaboration across governments, the technical community, and industry—no single actor can do this alone.”

He also pointed to the importance of focusing on key infrastructure layers—routing, DNS, and email—as the foundation for trust, aligning closely with the structure of the workshop itself.

Maarten Botterman, moderating the session, brought these perspectives together by emphasizing the fundamental structural challenge: the Internet was not originally designed with security as a primary objective but to be stable and interoperable. While modern standards now exist to address the security gap, their adoption remains uneven across regions and sectors.

He framed the workshop as part of a broader effort to address this imbalance: moving from availability of solutions to their consistent implementation, and from implicit trust to justified, verifiable trust.

The Technical Foundations of Trust: Today's Open Internet Standards

The first substantive session of the workshop focused on the technical foundations of trust in the Internet. While the Internet has evolved into critical global infrastructure, its core protocols were not originally designed with security as a primary objective. As a result, trust has historically been implicit—an assumption that is increasingly no longer tenable.

What emerged clearly from the discussion is that the building blocks for a more trustworthy Internet already exist. However, their deployment remains uneven, and their combined effect is only realized when implemented consistently across the ecosystem. The session therefore explored how modern standards in routing, naming, and email can collectively strengthen what may be understood as the Internet's "trust stack".

Routing Security – Establishing Trust in How Traffic Flows

The discussion began with routing security, where the limitations of the current system were articulated in practical terms. The Border Gateway Protocol (BGP), which underpins global Internet routing, was designed in a very different era—one in which networks largely trusted each other by default.

As Sunny Chendy (APNIC) explained: *“RPKI allows us to answer a fundamental question: is this network authorized to announce this prefix? Without that, we are still relying on trust assumptions that no longer hold.”*

The introduction of the Resource Public Key Infrastructure (RPKI) represents a significant step forward. Through Route Origin Authorizations (ROAs), network operators can declare which Autonomous Systems are authorized to originate specific IP prefixes. This provides a verifiable basis for trust—at least at the level of route origin.

Yet, as became evident in the discussion, authorization alone is not sufficient. For RPKI to have operational impact, networks must actively validate routing information through Route Origin Validation (ROV). It is here that a gap emerges: while the creation of ROAs is steadily increasing, the enforcement of validation remains limited. In practice, this means that the infrastructure may appear more secure than it actually is.

Building on this, Anurag Bhatia (Hurricane Electric) introduced ASPA (Autonomous System Provider Authorization) as an important next step in the evolution of routing security. While RPKI and ROA address the question of *who* is authorized to originate a route, ASPA addresses *how* that route propagates through the network.

As he noted: “ROA tells you who can originate a prefix. ASPA helps you understand whether the path the route took to reach you is valid. Together, they move us closer to end-to-end routing assurance.”

This distinction highlights an important progression: from origin validation to path validation. Together, ROA, ROV, and ASPA provide complementary layers of assurance, addressing both the legitimacy of announcements and the integrity of routing paths.

Despite these advances, the discussion made clear that routing security remains a collective action challenge. The benefits of deployment are shared globally, while the perceived risks and operational burdens are local. Overcoming this imbalance will require continued collaboration, awareness, and coordination—supported by initiatives such as MANRS.

DNS Security – Ensuring Trust in Where We Go

The discussion then moved to the Domain Name System, which acts as the Internet’s directory service. If routing determines how traffic flows, DNS determines where it goes. Compromise at this layer can redirect users to unintended—and potentially malicious—destinations.

Adiel Akplogan emphasized the centrality of DNS to trust: “If users cannot trust that a domain name leads to the correct destination, the entire system of online interaction is undermined.”

DNSSEC provides a mechanism to address this risk by enabling cryptographic validation of DNS responses. It ensures that the information received by users has not been tampered with and originates from the correct source.

However, as with routing security, the existence of the standard does not guarantee its effective deployment. While DNSSEC has seen strong adoption at the top-level domain level, its implementation further down the chain remains uneven. Operational complexity, concerns about misconfiguration, and limited awareness continue to hinder broader uptake.

To address this, the role of KINDNS was highlighted. Rather than introducing new technical standards, KINDNS focuses on operationalizing existing ones—encouraging consistent implementation through best practices, self-assessment, and knowledge sharing.

“The challenge is no longer defining standards, but ensuring they are implemented correctly and consistently across the ecosystem.”

This shift—from defining standards to embedding them in operational practice—represents a key step toward improving DNS resilience and trustworthiness.

Email Security – Ensuring Trust in Communication

The final part of Block I focused on email security, where the consequences of insufficient trust are perhaps most visible to end users.

Maarten Botterman explained that email remains one of the most widely used communication tools on the Internet, yet it was originally designed without built-in authentication mechanisms. As a result, it is inherently vulnerable to spoofing and impersonation. Standards are in place, yet, for instance, *SMTP (Simple Mail Transfer Protocol) allows anyone to send email on behalf of anyone else.*

To address this, a set of complementary standards has emerged over time. SPF (Sender Policy Framework) identifies which servers are authorized to send email on behalf of a domain. DKIM (DomainKeys Identified Mail) adds cryptographic signatures to ensure message integrity. DMARC (Domain-based Message Authentication Reporting & Conformance) builds on both by introducing alignment and policy enforcement, as well as reporting capabilities.

A key insight from the discussion was that these mechanisms must be understood as a progression rather than as independent solutions. SPF or DKIM are important, but alone won't protect against spoofing. DMARC provides the enforcement layer that turns authentication into protection.

In practice, however, full deployment remains challenging. While SPF and DKIM are widely implemented, DMARC is often deployed in monitoring mode without enforcement (“p=none”) which should only be a first step towards real protection by quarantining (“p=quarantine”) and ultimately rejecting (“p=reject”) invalidated messages . Moving toward full protection requires organizations to gain visibility into their email ecosystems, identify legitimate sending sources, and progressively tighten policies. According to Maarten Botterman it is only a matter of time until this is fully implemented as threats of abuse of email is going up by the day. Question is: will people wait until they really get compromised, or be ahead of that and implement solid measures before that happens?

Concluding: a Layered Understanding of Trust

Taken together, the discussions in Block I highlighted the interdependence of different layers of the Internet infrastructure.

Routing security ensures that data travels along legitimate paths. DNS security ensures that users reach the intended destination. Email security ensures that communications are authentic and trustworthy.

Each layer addresses a different aspect of trust, but none is sufficient on its own. Weakness in any one layer can undermine the overall system.

The overarching conclusion of the session was therefore both simple and profound:

*The Internet must evolve from implicit trust to verifiable, measurable,
and enforced trust—across all layers of its infrastructure.*

While the technical standards required to achieve this transformation are already available, their impact will depend on the willingness and ability of stakeholders to implement them consistently and at scale.

From Standards to Practice: Learning from What Works

Where the previous discussion focused on the technical foundations of trust, the discussion shifted to attention to real-world implementation, demonstrating how these standards and principles are being applied in practice across different layers of the Internet ecosystem.

A key theme throughout this session was that trust does not emerge automatically from standards alone. Rather, it is the result of intentional design choices, governance frameworks, and coordinated operational practices.

Trusted Domains and Architectures – Embedding Trust by Design

The session opened with concrete examples from the financial sector, where the need for trust is particularly acute.

From the Indian perspective, Dr. Devesh Tyagi, CEO of NIXI, introduced the concept behind .bank.in & .fin.in as a trusted namespace for financial institutions. The initiative is designed to provide users with a clear and reliable signal of authenticity in an environment where phishing and impersonation are increasing.

He emphasized the importance of combining technical controls with governance:

“With [.bank.in](#) & [.fin.in](#), we are creating a space where trust is not assumed, but verified. Only authenticated institutions can participate, giving users confidence that they are interacting with legitimate entities.”

This approach reflects a broader shift from open but ambiguous naming environments toward curated, policy-driven namespaces that reduce risk for end users.

This perspective was reinforced at the global level by Craig Schwartz, CEO of fTLD Registry, who shared the experience of operating .bank and .insurance as restricted top-level domains for financial institutions worldwide.

He highlighted the importance of embedding security requirements directly into the operational model:

“.bank was designed with security at its core—from strict identity verification to mandatory security controls. This creates a trusted ecosystem where both institutions and customers benefit from a higher level of assurance.”

Together, these examples illustrate how namespace governance can act as a powerful security mechanism, complementing underlying technical standards.

The session then turned to infrastructure-level innovation, with Nicola Rustignoli presenting the SCION secure network architecture that offers operational resilience in

highly critical connected ecosystems such as payments networks. SCION is currently serving the Swiss financial sector with a secure multi-operator communication facility.

SCION takes a fundamentally different approach by embedding security directly into the routing architecture, rather than layering it on top of existing protocols. It enables path awareness, cryptographic validation, and multi-path routing, offering enhanced resilience for critical systems.

As he explained:

“If we want to trust the network, we need to know not only where traffic comes from, but how it gets to us. SCION gives us that visibility and control.”

This represents an important evolution in thinking: from securing components of the Internet to re-architecting trust into the network itself, particularly for high-value and high-risk environments such as financial services.

Global Operational Communities – Scaling Trust Through Cooperation

The next part of the discussion highlighted the importance of global operational communities in sharing practice experiences and addressing systemic challenges it is not only about technical measures but also about operational practice.

Andrei Robachevsky, representing the Global Cyber Alliance, presented MANRS (Mutually Agreed Norms for Routing Security) as a response to the inherent collective action problem in routing security.

He emphasized that while technical solutions exist, their effectiveness depends on widespread adoption:

“Routing security is not something one network can solve alone. MANRS is about creating a shared baseline of responsible behaviour that, when adopted collectively, strengthens the entire Internet.”

MANRS provides a framework for networks to commit to best practices, including filtering, anti-spoofing, coordination, and transparency. Its success lies not in enforcement, but in community-driven accountability and shared norms.

Complementing this, Adiel Akplogan (ICANN OCTA) presented KINDNS, which applies a similar philosophy to DNS operations. Rather than focusing on new standards, KINDNS promotes the consistent implementation of existing ones through best practices and knowledge sharing.

He positioned both initiatives within a broader perspective:

“MANRS and KINDNS show that we can build global communities around good practice. These are networks of trust—where operators learn from each other and improve together.”

What Can Be Learned – From Standards to Scalable Trust

Across these contributions, several important lessons emerged.

1. Trust can be engineered in different ways. It can be embedded in:

- namespaces (e.g., .bank, .bank.in, .fin.in)
- network architectures (e.g., SCION)
- operational norms (e.g., MANRS, KINDNS)

Each approach addresses a different dimension of the trust challenge, but all share a common principle: trust must be made explicit and verifiable.

2. Governance and technology are inseparable. Technical mechanisms alone are insufficient without the policies and processes that ensure their correct and consistent application. The examples of .bank and .bank.in clearly demonstrate how governance frameworks can enhance the effectiveness of technical controls.
3. Collaboration is essential. Initiatives such as MANRS and KINDNS highlight that many Internet security challenges are inherently collective. Progress depends on building communities of practice that enable coordination, knowledge sharing, and mutual reinforcement.
4. Sectoral approaches can accelerate adoption. The financial sector, with its strong incentives for trust and risk management, has demonstrated how targeted initiatives can lead to rapid and meaningful improvements. These models can potentially be adapted to other sectors.
5. The transition from standards to trust requires operationalization at scale.

The tools, frameworks, and examples are already available. The challenge now lies in replicating and adapting these good practices across regions, sectors, and layers of the Internet ecosystem.

The path toward a more trustworthy Internet is not hypothetical—it is already being realized in practice. Through trusted namespaces, secure architectures, and global operational communities, stakeholders are actively building mechanisms that enhance trust, reduce risk, and improve resilience.

The key question going forward is not whether these approaches work, but how they can be scaled, adapted, and adopted more broadly to benefit the global Internet community.

Trust is achieved not only through technology, but through governance, coordination, and shared responsibility.

Planning for a More Trusted Internet: Marketplace for Action

The final block focused on translating insights into practical action. A central conclusion was that the main challenge is no longer awareness or availability of solutions, but deployment at scale. While standards such as RPKI, DNSSEC, and DMARC are well established, their implementation remains uneven.

Participants emphasized that progress requires institutional commitment, incentives, and accountability.

From Knowledge to Implementation

The moderator framed the discussion with a key observation: *“The knowledge exists, the tools exist, and the standards exist. The real question now is how to make adoption the default.”*

Ram Mohan (SSAC Chair and Chief Strategy Officer, Identity Digital) reinforced the systemic nature of trust:

“Trust on the Internet is not an abstract concept—it is instantiated in the infrastructure. Every domain name resolution, every routing decision, every email transaction is either reinforcing trust or eroding it. What matters now is ensuring that the secure path becomes the normal path.”

He emphasized that trust must be measurable and observable, supported by transparency and reporting.

Anand Raje presented the Trusted India Internet Initiative (T3i) was presented as a concrete step toward operationalization. The platform aims to test and monitor website and service security; provide visibility into compliance; support adoption of standards; and empower users and organizations. Early demonstrations showed both strong potential and significant gaps in implementation.

Martin Kuechenthal (CEO, LEMARIT) emphasized operational integration:

“Security must not remain an optional add-on. If we want meaningful progress, security needs to be embedded into default configurations—at registrars, hosting providers, and platforms.”

This highlights the critical role of registries and registrars in normalizing secure configurations at scale, and the necessity to see this as a justified business investment.

Participants explored how governance frameworks can accelerate adoption, focusing on baseline expectations for critical sectors procurement requirements including

security standards; leadership by example from governments; and effective recognition mechanisms for compliance. Trusted namespaces such as .bank demonstrate how governance and enforcement can create higher trust environments.

Community, Sustainability, and Scale

The importance of community-driven initiatives was widely recognized, alongside the need for sustainable models. Scaling requires stable funding, institutional support, clear governance and continuous stakeholder engagement

Collaboration between initiatives such as T3i, MeitY, NIXI, CDAC, and global communities (GFCE, GCA, MANRS, KINDNS) was identified as essential.

This is important as user awareness is a key driver for change. By enabling users to assess security, these platforms can create informed demand and drive provider accountability by enabling market differentiation based on trust and incentivising a continuous process of improvement.

The session concluded with a shared recognition:

“Trust emerges from the combined actions of all stakeholders.”

The fundamental shift we are looking at to *ensure justifiable trust* is:

- from optional → default security
- from fragmented → coordinated action
- from awareness → measurable implementation

Closing

On behalf of GFCE Triple-I, sincere thanks to all contributors. Thanks to all participants, including global and regional experts from government, industry, academia, and the technical community. The hybrid format enabled active engagement and exchange of perspectives.

Special thanks to:

- Sushil Pal (Joint Secretary, MeitY)
- NIXI (Dr. Devesh Tyagi, Sameer Gahlot) for hosting
- ICANN and supporting partners
- Speakers from APNIC, ISOC, Global Cyber Alliance, EasyDMARC and others
- Local coordinators and volunteers

The workshop reaffirmed that The Internet's trustworthiness depends on collective action.

Technical solutions are available, but their impact depends on adoption, coordination, and sustained collaboration. GFCE Triple-I and initiatives such as T3i, MANRS and KINDNS provide a pathway to translate knowledge into action and strengthen justified trust in the Internet and email.

--(O)--

Big thanks to NIXI for hosting the workshop, fTLD for sponsoring lunch and refreshments, and EasyDMARC for contribution to travel costs. It would not have been possible to gather without you.

--(O)--

For more information about GFCE Triple-I, including results of earlier events, please check out the [GFCE website](#). Contact [Maarten Botterman](#) if you have specific questions about GFCE Triple-I, and if you are interested in improving the trusted Internet experience in your region.

GFCE Triple-I Mumbai, India

ICANN 85, Jio Centre, 8 March 2026

09:30 Registration & coffee/tea

Registration and opportunities for catching up with other participants.

10:00 Opening by Host and Moderator: Welcome and intent of the day

Word of welcome by Vint Cerf. Opening by Shri Sushil Pal (Joint Secretary, Indian Ministry for Electronics and IT), welcoming words from Nico Caballero, Chair of the ICANN Government Advisory Committee, and introduction to the day by Maarten Botterman (GFCE Triple-I coordinator).

10:30 Block I: Better Use of Today's Open Internet Standards:

Moderated discussion about the use and usefulness of modern Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF.

- Routing Security (RPKI, ROA, ASPA). Speakers: Sunny Chendi (APNIC); Anurag Bhatia (HE).
- DNS Security (DNSSEC, DANE, TLS). Speaker: Adiel Akplogan (ICANN)
- E-mail Security (DMARC, DKIM, SPF). Speaker: Hagop Khatchoian (EasyDMARC)

These standards are also discussed in the [GFCE Triple-I Handbook](#), and technical tests for the state of implementation are available at www.internet.nl (Dutch and English).

12:00 Break – light lunch and refreshments (*offered by fTLD*)

13:00 Block II: Inspiration from Good Practice Action: focus on trusted online financial services MANRS; and setting standards

During this Block, we talk about ongoing initiatives in India and the world that may inspire specific action with a focus on secure financial services from India and around the world. Focus for this workshop will be on

1. secure financial services with input from organizations active in this:
 - o [NIXI](#) (as NIXI is deploying a secure BANK.IN domain. Speaker: Dr. Devesh Tyagi, NIXI CEO;

- [SCION](#) (as SCION has provided a secure solution for the Swiss banking world; Speaker: Nicola Rustignoli, SCION)
 - [fTLD](#) Registry (as fTLD registry provides secure domains under dotbank and dotinsurance TLDs). Speaker: Craig Schwartz, fTLD.
2. Global community activity for secure routing MANRS: what does it do and how does it do it. Speaker: Andrei Robachevsky, Global Cyber Alliance
 3. Update on KINDNS: Speaker; Adiel Akplogan (ICANN)

15:00 refreshments in the room

15:15 Block III: Planning for a More Trusted Internet: Marketplace for Action

Facilitated brainstorm, based on the input discussed over the day, and an introduction on a possible way forward leveraging the “justified trust in the use of the Internet and email” throughout the region.

With inputs from , Ram Mohan, Chair of ICANN Security and Stability Advisory Council, Martin Kuechenthal, CEO of LEMARIT, Anand Raje, Coordinator of T3i, and open floor to all.

At the end of the day the moderator Maarten Botterman (GFCE moderator) will summarize initial findings in interaction with all participants, and close the day with thanks to all participants.

Annex 2 - Contributing organizations

Workshop organizer

The [Global Forum on Cyber Expertise \(GFCE\)](#) is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. This is the 14th Triple I workshop under the GFCE auspices.

Workshop host

The [National Internet Exchange of India \(NIXI\)](#) is a non-profit company incorporated under Section 25 of the Indian Companies Act, 1956 with an objective of facilitating improved internet services in the country.

Expert input

The [Internet Corporation for Assigned Names and Numbers \(ICANN\)](#) is a global multistakeholder group and nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet while also ensuring the Internet's secure and stable operation.

The [Asia Pacific Network Information Centre \(APNIC\)](#) is an open, membership-based, not-for-profit organization providing Internet addressing services to the Asia Pacific.

The [Global Cyber Alliance \(GCA\)](#) mobilizes collective action to tackle the Internet's greatest challenges and build a safer digital world for everyone. Its work includes development, coordination and support of the [MANRS](#) initiative and its community to improve routing security."

[EasyDMARC](#) is a cloud-native email authentication and deliverability platform designed to simplify email authentication and deliverability management. Deliverability should not be confused with delivery: deliverability rate is a percentage of how many emails actually reach the inbox because they are trusted.

[SCION](#) is a Switzerland-based non-profit organization driving transformation of the Internet infrastructure with SCION technology aiming at a future where the exchange of information can be made trustworthy; anytime, anywhere and for anyone.

[fTLD Registry Services \(fTLD\)](#) operates .Bank and .Insurance. The global banking and insurance communities created these top-level domains to shield against cyberattacks, fraud, and impersonation. fTLD is governed by leading financial services organizations Protected by strict registration requirements and mandatory Security Requirements since its establishment in 2011.

--(O)--