GFCE Global Good Practices

Internet Infrastructure Initiative (Triple-I) 2025

Preface

The economic growth and social benefits that were boosted by the internet require a sustained trust in the cyber domain. This level of trust is being threatened by cyber-attacks (e.g. hacking, denial of service attacks), cybercrime (e.g. ransomware, spoofing) and unwanted messages (e.g. spam). The global exposure of these threats requires a collaborative response to build capabilities that improve internet security.

A foundation for internet security is provided by the ecosystem of protocols, standards, technology, practices and organisations that are the internet's infrastructure. An important contribution to a secure and resilient internet infrastructure is the adoption and deployment of open, security-oriented internet standards. Initiatives to promote the use of these standards have been initiated and supported by organisations around the world. In addition, practices have been put in place to address internet and e-mail related threats around the world – practices that could inspire action in other parts of the world, as well.

More wide-spread collaboration and extension of these initiatives are required to reap the benefits of a secure internet. The GFCE Internet Infrastructure Initiative (III) is to bring stakeholders together, raise awareness and provide support for world class standards and practice deployment in the regions. This initiative build on global and local cooperation, and benefits from the availability of a website to raise awareness and to test standards-compliance (www.internet.nl).

This Global Good Practice on Internet Infrastructure helps policy-makers, political and business leaders in defining sustainable and efficient efforts to stimulate adoption of open internet standards. It helps Internet Service Providers to understand how service can be made up-to-standard at least, or better, and it helps users (businesses, individual users) to better understand what practices to adopt to be safer, and what to ask for from their service providers and governments. This document provides both a recommendation relating to adoption of state-of-the-art internet standards that make the Internet and e-mail infrastructures more robust in their use, and a set of good practices to develop an effective national and regional internet infrastructure deployment program, that is aligned in the international Internet Infrastructure Initiative.

This Handbook could not have been written without the support and input from a number of organizations, and our deep thanks go out to them. To TNO for creating the first version of this

Handbook in 2016. To those who contributed by providing input and suggestions from ICANN, Internet Society, Global Cyber Alliance, RIPE NCC, APNIC, LACNIC, AFRINIC, SCION Association, EasyDMARC, Dutch Platform Internet Standards, M3AAWG, and all participants to the GFCE Triple-I events around the world.

And to the GFCE community that had the vision to support this activity from its first meeting onward, hosted by the African Internet Summit on 16 June 2016 in Kampala, Uganda.

Maarten Botterman
GFCE Triple-I coordinator
Rotterdam, August 2025

1. Introduction

1.1 Internet infrastructure & internet standards

Internet infrastructure is the ecosystem of protocols, standards, technology, practices and organisations that keep the internet running. An open, stable and secure internet infrastructure is key to sustaining the economic growth and social benefits that were boosted by the internet. These internet-driven innovations require the continuation and improvement of trust in the cyber domain that is threatened by cyber-attacks (like Distributed Denial-of-Service attacks), cybercrime (hacking, malware, phishing, botnets, ransomware) and unwanted messages (like (e-mail) spam or e-mail as a vehicle to engage in cybercrime). The global exposure of these threats requires a collaborative, global response to secure the internet infrastructure to sustain the benefits of the internet.

An important contribution to a secure and resilient internet infrastructure is the adoption and deployment of security-related internet standards. An Internet standard is a specification that has been approved by the Internet Engineering Task Force (IETF). An IETF Internet Standard is a voluntary standard characterised by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefits to all stakeholders of the Internet community. The adoption of these standards helps to promote a consistent, universal and secure use of the internet worldwide.

Next to that, adoption of good practices helps further enhance “justified trust in the use of the Internet and e-mail” within regions when deployed in that region– and all this through raising awareness and inspiring local and regional multistakeholder communities to collaborate based on that recognition of good practice.

1.2 The GFCE Internet infrastructure initiative (GFCE Triple-I)

The effectiveness of security-related and other key internet standards as well as good practices increase with the scale of their adoption. Therefore, their adoption requires collective action by key stakeholders, including government, industry, civil society and the technical community, both globally and regionally. The Internet Infrastructure initiative aims to bring stakeholders together, globally and regionally, to raise awareness and provide support to all stakeholders with the deployment of internet standards and related technologies to help ensuring (continued?) justified trust in the use of the Internet and e-mail.

The internet infrastructure initiative (Triple-I) promotes the use of the following internet standards:

- **IPv6**: a major extension of the internet address range and enabler of security capabilities
- **DNSSEC**: security extensions for the internet domain name infrastructure
- **TLS, HTTPS, DANE and STARTTLS**: secured connections between internet users and services
- **RPKI, ROA**: helps prevent route hijacking and other routing attacks through use of trust anchor;
- **DKIM, SPF and DMARC**: anti-phishing and anti-spoofing measures

The Triple-I initiative aims to bring awareness to the regions of the standards above and what they can bring in terms of enhanced trust in the local use of the internet and e-mail. It can be expanded with information on good practices aiming at building or improving the key elements that enable a properly functioning internet in each country, such as neutral IXPs (Internet Exchange Points), running a national domain registry (ccTLD), development of open source software, and routing security (MANRS). Furthermore, ICANN developed the Domain Abuse Activity Reporting (DAAR) project, which set up a system for studying and reporting on domain name registration and security threat (domain abuse) behavior across top-level domain (TLD) registries, and KINDNS, an initiative to promote voluntary security best practices for authoritative and recursive DNS operators.. These activities are complementary to the Internet Infrastructure Initiative, and can be seen as global good practices that can further support local and regional communities enhance justified trust in the region.

1.3 Goal and outline of this document

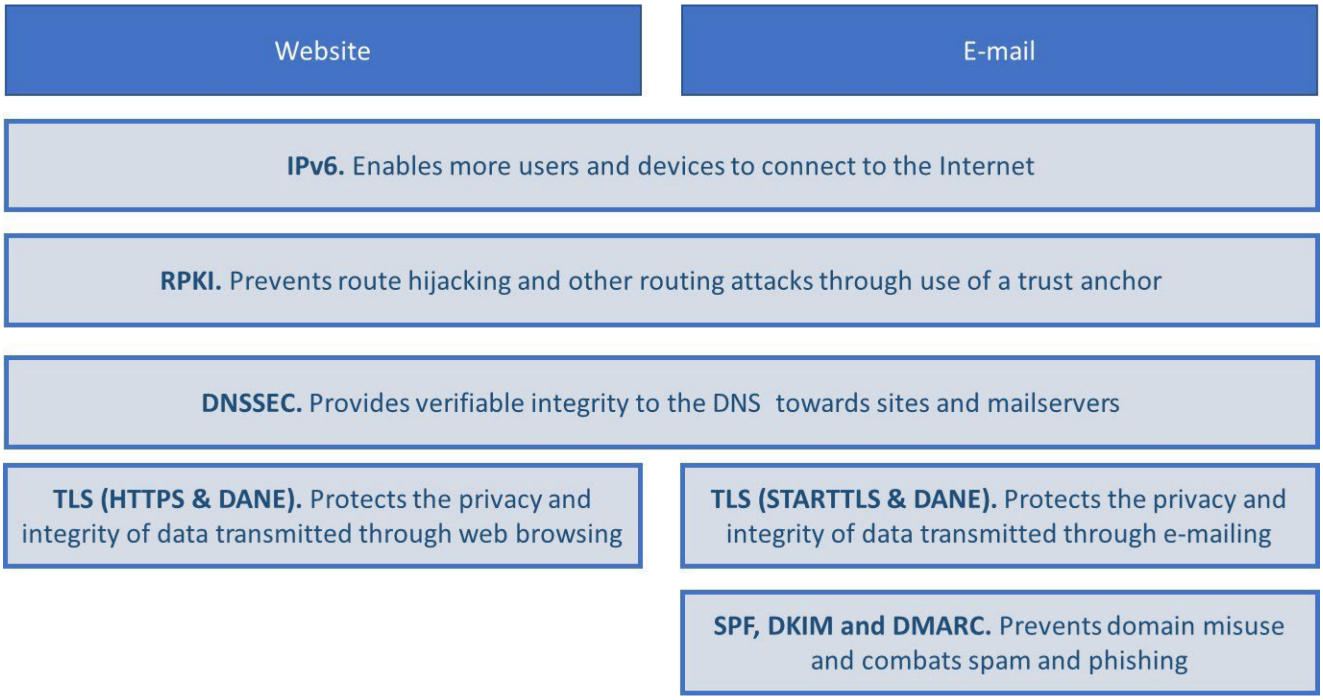
This document describes the good practices which can be part of an internet infrastructure initiative. The target audience comprises public policy-makers, who can use these good practices to develop a (national) policy or strategy for developing III programs. The content of this document is prepared for policy-makers that have basic knowledge of the internet infrastructure, but are no expert in the field. It also benefits Internet Service providers that want to ensure providing the current best practice services to their customers, as well as users, to know what services to look for from their providers.

In the next chapter, a high-level overview on the internet standards that are in the current scope of the initiative is given. Chapter 3 presents a set of good practices that help enhance justified trust in the use of internet and e-mail. Chapter 4 contains more background information on the standards, including a high-level description of the technical workings, the benefits that they provide, the current global adoption rates, and the challenges which need to be overcome when promoting these standards.

2. Background internet standards

This chapter outlines the security-related Internet standards promoted through Triple-I that fall within the scope of this document. These open standards are developed by the Internet industry and published by the Internet Engineering Task Force (IETF, 2017). For a more detailed discussion—including benefits, challenges, and adoption status—see Chapter 4.

Figure 1 illustrates how the selected standards interrelate.



Website

E-mail

IPv6. Enables more users and devices to connect to the Internet

RPKI. Prevents route hijacking and other routing attacks through use of a trust anchor

DNSSEC. Provides verifiable integrity to the DNS towards sites and mailservers

TLS (HTTPS & DANE). Protects the privacy and integrity of data transmitted through web browsing

TLS (STARTTLS & DANE). Protects the privacy and integrity of data transmitted through e-mailing

SPF, DKIM and DMARC. Prevents domain misuse and combats spam and phishing

Figure 1: Overview of the internet standards in scope

These Internet security standards protect different layers of online communication, from routing and addressing to name resolution, transport encryption, and e-mail authentication. They are complementary rather than standalone. Below we further define purpose and application of the standards

➢ 2.1 TLS & HTTPS

These standards protects the privacy and integrity of transmitted data. Transport Layer Security (TLS) encrypts data transmitted between two endpoints (e.g., a user and an online service), ensuring confidentiality and integrity. Its most common application is securing website interactions through

HTTPS—identifiable by the “lock” icon in the browser address bar and URLs beginning with https:// rather than http://.

TLS is also used in securing e-mail transport and other Internet applications. By verifying the authenticity of the remote service, TLS helps prevent data interception, tampering, and impersonation. Given the sensitive nature of online transactions, TLS is essential to privacy and trust.

Two related mechanisms strengthen TLS:

- DNS-based Authentication of Named Entities (DANE) – Adds cryptographic assurance via DNSSEC to TLS certificates.
- STARTTLS – Enforces TLS encryption in protocols like e-mail transmission.

2.2 DNSSEC

DNSSEC provides verifiable integrity to the DNS towards sites and mail servers and prevents the redirection of internet users to malicious sites or mail servers. Domain Name System Security Extensions (DNSSEC) verify the authenticity and integrity of DNS data. Without DNSSEC, attackers could manipulate DNS responses, redirecting users to malicious websites or mail servers.

DNSSEC prevents such redirection by cryptographically signing DNS data, ensuring that IP addresses and other DNS information are legitimate. While it cannot stop users from visiting harmful sites via deceptive links, DNSSEC is a critical safeguard for all Internet services—not only websites, but also e-mail, instant messaging, and VoIP. It also underpins other security protocols such as DANE.

2.3 RPKI & ROA

Internet routing uses the Border Gateway Protocol (BGP), which is vulnerable to route hijacking and misdirection. The Resource Public Key Infrastructure (RPKI), defined by the IETF, provides a secure way to verify ownership of Internet number resources (such as IP addresses) through a trust anchor.

A key operational element of RPKI is the Route Origin Authorization (ROA). ROAs are digitally signed statements that specify which Autonomous Systems (AS) are authorized to originate routes for particular IP address blocks. Network operators use ROAs to validate BGP route announcements, reducing the risk of route hijacking and accidental misconfiguration.

By combining RPKI with ROA validation, legitimate resource holders can control the operation of Internet routing protocols and improve the global security and stability of routing.

2.4 SPF, DKIM & DMARC

These standards help prevent domain misuse and combat spam and phishing. E-mail by default does not authenticate the sender address, enabling malicious actors to "spoof" messages that appear to come from trusted domains. This undermines spam and phishing defenses.

Three complementary standards provide sender authentication:

- SPF (Sender Policy Framework) – Specifies which mail servers are allowed to send e-mail for a domain.
- DKIM (DomainKeys Identified Mail) – Cryptographically signs e-mails to verify they have not been altered and originate from authorized servers.
- DMARC (Domain-based Message Authentication, Reporting & Conformance) – Builds on SPF and DKIM, allowing domain owners to set handling policies for failed authentication and receive detailed reports.

Together, these standards help organizations detect and block fraudulent e-mail.

2.5 IPv6

Each Internet-connected device requires a unique IP address. The widely used IPv4 protocol provides about 4.3 billion addresses, nearly all of which are allocated. IPv6 expands the address space to trillions, enabling continued growth of the Internet and the proliferation of connected devices.

IPv6 also improves routing efficiency, supports better end-to-end security, and removes certain limitations of IPv4, making the Internet more scalable and resilient.

2.6 Interrelation and dependencies

The security-related Internet standards described in this document form a complementary framework. Each addresses a different layer of Internet communication, but their effectiveness increases when deployed together. TLS/HTTPS protects data in transit, while DNSSEC ensures that the domain names used in TLS certificates and other services resolve to the correct IP addresses. DANE bridges DNSSEC and TLS, allowing cryptographic credentials to be securely published in the DNS.

RPKI, supported by Route Origin Authorizations (ROAs), protects the routing layer by preventing misdirection of traffic before it reaches the intended IP address. DNSSEC and RPKI together strengthen trust in both name resolution and network path selection.

In the application layer, SPF, DKIM, and DMARC depend on accurate DNS records—whose integrity can be guaranteed by DNSSEC—to authenticate e-mail senders and block spoofing. Similarly, STARTTLS relies on TLS to secure e-mail in transit.

Finally, **IPv6** underpins the long-term scalability of all these standards by providing sufficient addressing space and enabling more efficient, secure network operations. Full protection depends on coordinated deployment: end-user devices, servers, DNS infrastructure, and routing systems must all implement the relevant standards for security to be comprehensive

In Chapter 4 we expand specifically on what this means for Routing Security; DNS Security; and e-mail security.

➢ 2.7 Preparing for the future

Even when we have implemented all measures possible today, it will be important to think ahead in the light of technology developments. Each of these technologies comes with opportunities and threats, and whereas it is not in the scope of this document to either predict the future or present the forefront of developments, it is important to be aware of the following potential threats:

2.7.1 Quantum computing

Quantum computing is progressing fast enough that today’s public-key cryptography (RSA, elliptic-curve) will not remain secure indefinitely. Even before a large, fault-tolerant quantum computer exists, adversaries can harvest encrypted data now and decrypt it later (“HNDL/SNDL”). That creates long-tail risk for any data with multi-year sensitivity (e.g., personal data, trade secrets, health and financial records, industrial IP, critical infrastructure telemetry).

In particular, the following threats relate to Quantum computing

- Confidentiality break of public-key crypto. Practical quantum attacks (Shor’s algorithm) would break RSA/ECDH/ECDSA, compromising TLS handshakes, VPNs, S/MIME, PGP, code-signing, and device onboarding flows. Integrity and authenticity guarantees relying on those schemes would also fail. (ENISA[1])

- Harvest-now, decrypt-later exposure. Data captured today (e.g., database backups, network captures, satellite downlinks) could be decrypted retroactively, turning "older" breaches into impactful future disclosures[2].
- Long-lived systems & data. OT/ICS, medical, automotive, aerospace, and IoT deployments with 10–20-year lifecycles, and records with long confidentiality needs, are especially at risk. (Regulators and standards bodies increasingly expect forward-secrecy and crypto-agility for these contexts.) (EU Digital Strategy)
- Supply-chain and protocol ossification. Hard-coded algorithms, inflexible certificate formats, and brittle APIs make migration slow—creating a window of heightened risk during transition. ENISA and NIST emphasize crypto-agility as a design prerequisite.

The global response is underway. In 2024, NIST published the first post-quantum cryptography (PQC) standards: ML-KEM (a key-establishment KEM; based on Kyber) and ML-DSA (a signature scheme; based on Dilithium), plus SLH-DSA (hash-based SPHINCS+). Additional work continues across IETF for hybrid TLS 1.3 key exchange (classical + PQC in one handshake), and governments have set transition timelines (e.g., NSA CNSA 2.0 targets PQC protection for U.S. national security systems by 2035, with milestones starting this decade). The EU has issued a coordinated PQC migration roadmap. These signal that planning must start now, not "when Q-day arrives." (NIST[3], IETF Datatracker[4], U.S. Department of Defense[5], EU Digital Strategy[6]).

2.7.2 Artificial Intelligence

AI is already embedded in strategic decisions, customer interactions, software development, and security operations. The upside is large—but so are the risks, including new attack surfaces (prompt injection, data poisoning), regulatory exposure, and reputational harm from misuse (e.g., deepfakes). Governments and standards bodies have moved from principles to concrete guidance (EU AI Act, NIST

[1] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
[2] https://cypfer.com/harvest-now-decrypt-later-the-quantum-threat-that-has-already-begun/
[3] https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process
[4] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
[5] https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
[6] https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

AI RMF, ISO/IEC 42001, G7 Code of Conduct), so organizations need a pragmatic plan that aligns innovation with governance and security from the outset.

It will be important to treat AI like aviation: innovation with disciplined safety. The opportunity is real, but so is the obligation to engineer, monitor, and govern systems against misuse and error. It is build secure-by-design systems, and align to emerging standards such as the NIST AI Framework, ISO/IEC 42001, and regulations such as the EU AI Act. It is not only about systems, but also about processes, and awareness raising and training of people to ensure a robust response.

2.7.3 Conclusion

Preparing for the future is not about predicting timelines; it is about reducing exposure to foreseeable risks while preserving the freedom to innovate. Quantum computing and artificial intelligence exemplify this dual imperative. Quantum progress threatens today’s public-key cryptography and can turn “harvest-now, decrypt-later” into tomorrow’s breach. AI, meanwhile, expands what is possible for service quality, security operations, and inclusion—yet also introduces novel failure modes, attack surfaces, and governance obligations. The common lesson is clear: resilience comes from planning early, engineering for agility, and building capable, informed teams.

For cryptography, that means moving from awareness to action: create a cryptographic inventory, map data with long confidentiality lifetimes, and design systems to swap algorithms without upheaval. Pilot hybrids and post-quantum primitives in controlled environments, refresh PKI and certificate profiles, shorten key lifetimes, and embed crypto-agility into architectures and procurement. This staged approach limits harvest-now risk today and accelerates an orderly transition as standards and implementations mature.

For AI, treat safety and integrity as first-class product features. Establish an operating model that assigns ownership, documents data lineage, and tests systems against realistic threats such as prompt injection, poisoning, and model leakage. Build secure-by-design controls into development and deployment, maintain human oversight where it matters, and align practices with emerging frameworks and laws. Training, red-teaming, logging, and incident playbooks convert policy into operational muscle.

Finally, measure and collaborate. Set short, public milestones; use conformance and testing tools; require vendor roadmaps; and share lessons across communities. By coupling disciplined governance with practical engineering and ongoing capacity building, organizations can capture AI’s benefits, prepare for quantum disruption, and keep users’ trust at the center of a modern, open, and secure Internet.

3. Good practices

Good practices inspire action in other regions, where applicable, and customized by the stakeholders in that specific region for their specific situation. This chapter presents a set of good practices that may be useful to consider in order to pursue the objectives of Triple-I: *increasing justified trust in the use of the Internet and e-mail in the region*.

3.1 Good practice 1: Establish a national multi-stakeholder cooperation platform to identify appropriate action

A voluntary-based cooperation, which has a common goal and shared responsibility, can contribute to an increased level of internet security. Such a cooperation comprising various types of stakeholders encourages raising mutual awareness about the weaknesses in systems, discussing main challenges and solutions, and providing mutual support in taking preventive measures. This mechanism is transparent, triggers improvement, and its results are an incentive for organisations to increase efforts.

The cooperation contributes to the development of an enabling environment at the national level by raising the awareness for the need to implement available mature internet standards. All recent standards created by the Internet Engineering Task Force (IETF) include a specific security consideration section – yet adopting these standards is on a voluntary basis and needs to be seen as a priority. All this contributes to partnership building by creating mechanisms and frameworks for cooperation and collaborative learning. It therefore develops capacities of the participating stakeholders through cooperation, awareness raising, focused workshops and discussions, expert support and advice, exchange of resources, and development of guidelines for the deployment of the security-related and other key internet standards.

3.1.1 Actors (for who is this good practice document?)

The implementation of security standards is a collective effort by many organisations. The cooperation stimulates multi-stakeholder cooperation and sharing expertise.

A typical cooperation is comprised of technical Internet-related organisations and departments - the national Computer Security Incident Response Team (CSIRT), the Ministry or National Regulatory

Authority in charge of Internet policymaking, civil society (ISOC), the technical community (RIRs, ICANN) and umbrella organisations representing businesses in the ICT-sector: e.g. Internet Service Providers (ISPs), ICT solution providers, manufacturers, and hosting providers. There can also be other organisations that underpin and support the activities as long as their participation is not used to promote their own products or services.

3.1.2 What is the timeline for implementation?

The local environment and context highly influences the time scale for establishing such a cooperation. No general scheme exists, but experiences by other established cooperations may be of help. Drawing from practice in the Netherlands, it took about one year to set up an operational cooperation.

Once established, the lifetime of a cooperation depends on the initial goal; e.g. the cooperation could dissolve when a certain percentage of implementation has been achieved. In principle, the cooperation continues to be useful as long as implementation of the selected set of internet standards does not achieve a certain maturity. For certain standards this can take a long time. For instance, a similar Task Force for the promotion of IPv6 in the Netherlands still exists after about ten years, because of the slow pace of IPv6 adoption.

3.1.3 How can this be implemented?

Practical steps for implementation: principles & recommendations:

- Involve organisations and institutions particularly interested in improving the level of trust through the use of security related internet standards. Participation should have a low barrier - open to all stakeholders that support the mission and activities, and which will not use the cooperation for product promotion, marketing and direct sales.
- Prepare and agree a code of conduct and act on accordingly on a set of basic principles for participation.
- Find the most meaningful and feasible way of participation for each organisation. Organisations should contribute to the cooperation by allowing their employees to be involved in activities, such as hosting or facilitating meetings, or utilising their communication channels for outreach.
- Organise the cooperation in a lightweight 'organised network' rather than an organisation with headquarters, employees or formal partnerships.
- Avoid unnecessary overhead costs and bureaucracy. Ensure a basic budget - through contributions of several stakeholders and possibly the government - for basic support (active

chairperson, website and tools development, and secretariat functions). Other contributions should be in-kind by partners.

- Focus the discussions and work on technology - challenges and solutions – and limit the joint work to that rather than on broad aspects.

3.1.4 What are the challenges?

The following challenges can be identified:

- Different national approaches that need to be examined. In general, this cooperation works best in an environment that is already acquainted with multi-stakeholder initiatives. In environments that are not susceptible to a multi-stakeholder model, a different approach might be considered.
- The biggest challenge is in the initiating phase. Most organisations in the private sector acknowledge the need for action, but are not willing or do not feel the responsibility of taking the necessary first step.
- A possible extension of the cooperation beyond national borders would increase the number of requests for support, which conflicts with the voluntary, low-cost support activity of the cooperation. It is therefore better if the cooperation activities are adapted by different countries to make it locally-specific.

3.1.5 Application examples

Many cooperations with the task to promote internet standards already exist. Government agencies are responsible for the grand design, strategic planning and budgets. The industry and private companies develop R&D and trial projects. For the general public, the body writes press releases, organizes events and performs road shows. A consumer monitoring group provides feedback on products.

In the Netherlands, the “Platform for internet standards” promotes, amongst others, security-related internet standards:

- The Dutch government embraced the public interest of this initiative and became an active driving force to set up this cooperation. It gave initial funding (being a majority financial contributor) and gathered interests and participation. After two years, the Dutch government’s involvement in terms of money and time spent has decreased (but is still substantial) as a result of increased involvement by other (inter)national stakeholders. The cooperation focusses only on technical standards, as it mainly comprises technical organisations and departments.

- The Dutch Platform for internet standards organises two seminars or workshops a year for interested parties. The events are narrowly focused - such as on e-mail security - covering implementation practices and tools, preferably open source, and how various tools complement each other. It also published a paper on encryption and TLS that takes political aspects into account.
- Each year the number of companies and organisations that took part in the cooperation has increased. This is partially due to an increase in the use of the publicly provided testing tool (see: Good Practice 2 “Create an internet standards awareness website”). The positive competition to receive a ‘badge of honour’ on the testing tool webpage has improved implementation of internet security standards across the Netherlands. National implementations of the code have been adopted by other countries around the world.

➢ 3.2 Good practice 2: Create an internet standards awareness website

To stimulate awareness, enable and encourage individuals and organisations to use and deploy important internet standards, a website should be created. This website should provide information to motivate adoption and provide tools for testing compliance with these standards.

This website should be a free and public service. The visitor should find comprehensible supporting documentation about the internet standards, complemented with arguments and pitfalls regarding their deployment. Further, the visitor can - in real time - check any given domain name, whether used as a website or within an e-mail address, for standards-compliance. The test results include suggestions for taking next steps, such as the advice to contact one’s Internet provider to enable IPv6. The online tool may also act as a communication channel and point of contact for any national initiative related to the implementation of the various security-related and other key internet standards.

This tool contributes to the implementation of key internet standards through a variety of mechanisms:

- It raises awareness on key internet standards and provides implementation support.
- The rating system, based on testing tool results, triggers peer pressure.
- Decision-makers can get insights into the deployment-status of internet standards within their organisation and act on it.

- The press can use it to write about organisations who lack the necessary standards. This could have political impact. For example, the Dutch minister of the Interior promised to fix the poor security of municipal e-mail systems across the country after the press addressed this issue.

While the tool provides support for the implementation of internet standards, for most organisation this would not be sufficient and a more comprehensive approach is needed. A cooperation of organisations could provide the required support and it can be used to discuss the challenges which need to be overcome when implementing the standards (see: Practice "Establish a national multi-stakeholder cooperation to promote standards").

3.2.1 Actors (for who is this good practice?)

Targeted stakeholders are in general all organisations that heavily rely on the internet to communicate with users. Typically, these stakeholders are ISPs (access and e-mail), government authorities (e-governance) and the business sector (e-commerce). Yet anyone, including individuals, can use the test tool to check the level of implemented security-related internet standards in their own system.

3.2.2 What is the timeline for implementation?

Development of a website and a testing tool can run in parallel with setting up a cooperation (see: Practice "Establish a national multi-stakeholder cooperation to promote standards"), provided there is a small group of initiators willing to invest in it.

In the case of a straightforward duplicated/translated version of existing practices (see example below), it will take a couple of months to develop. When there are specific needs and adaptations required, the development can take up a year.

After the initial development, it needs to be improved and updated on a continuous basis (new functions, user feedback, bugs etc.). The goals of the platform determine how, and how long, the tools need to be used and therefore be maintained.

3.2.3 How can it be implemented?

Practical steps for implementation are:

- Register a simple domain that people can remember.
- Prepare instructions in a simple non-technical language.
- Create a communication platform to promote your tool (see: Practice "Establish a national multi-stakeholder cooperation to promote standards").

- Create a support team that will answer users' questions.
- Tailor the components of the website to your national context (e.g. multiple languages).

3.2.4 What are the challenges?

The following challenges should be considered:

- Lack of awareness, which could be mitigated through awareness-raising campaigns (using simple terminology, potentially showcasing metrics).
- Language barriers, which may be addressed through the translation of materials and developing local content.

3.2.5 Application Example

The awareness website and testing tool made available for the GFCE Internet Infrastructure Initiative is available at www.internet.nl. It is available in English and Dutch and can be used by stakeholders in any country, for any domain and any internet connection. The code is freely available from Github, and an international support community is developing.

Website statistics show that the testing tool is being used increasingly. The tool revealed a lack of use of key internet standards by several government organisations in the Netherlands. In response, the Minister in charge requested Dutch government organisations to adopt the proposed standards, or explain why this was not (yet?) possible – a “comply or explain obligation”. Overall this has led high adoption rates of these Internet standards throughout the Dutch government, further strengthened by including these standards a requirements in procurement processes. Other institutions and communities, such as the Brazilian CGI, have built websites using the testing code and integrating it in a regional API (see https://top.nic.br/).

3.3 Good practice 3: Provide economic incentives

For businesses, economic incentives are key motivators. Markets for internet access, domain registration, certification services, and cloud infrastructure offer ample opportunities for both economic and regulatory incentives that can accelerate adoption of important Internet security standards—such as IPv6, DNSSEC, TLS/DANE, RPKI/ROA, and e-mail authentication protocols (SPF, DKIM, DMARC).

Governments—possibly in collaboration with registries, registrars, public agencies, and service providers—should explore and tailor these incentives to regional economic conditions and policy environments.

Examples of effective economic incentives include:

1- Tax & Recognition Programs: South Korea and Japan have historically offered tax incentives and official “IPv6-ready” certifications to encourage infrastructure upgrades and market recognition—proving the effectiveness of financial and reputational rewards.
2- Registry–Registrar Discount Schemes: Not-for-profit ccTLD registries can offer fee discounts for domains that meet security requirements (DNSSEC, IPv6-enabled, etc.), as seen in France (AFNIC), Europe (.eu – EURid), Norway (NORID), and the Netherlands (SIDN). SIDN’s "Registrar Scorecard" rewards registrars based on DNSSEC and IPv6 adoption levels. The business interaction between these internet registries and registrars has been successfully used to stimulate open standard adoption.
3- Government procurement programs including specific cybersecurity requirements thus ensuring offering these secure services becomes an option on national markets. Clear examples include the Dutch government’s “comply or explain” policy requiring government agencies to adopt modern Internet standards; the US Gvoernment requirement to have at least 80% of IP-enabled assets in federal systems to run IPv6-only networks by the end of fiscal year 2025, driving both governmental and commercial adoption, and the Czech Act on Cybersecurity that makes DNSSEC compulsory for all public institutions, and DANE for their e- mail servers.

Governments leading by example by implementing the security-related and other key internet standards in existing systems and networks and through their procurement processes is a key activity, not only to ensure that the government services themselves are more secure, but also that there are commercial incentives to offer those secure services in the market. And many countries have already taken extensive measures to ensure government agencies lead by example.

➢ 3.4 Good practice 4: Capacity building workshops

Since 2018, GFCE has facilitated regional, multi-stakeholder **GFCE Triple-I** (Internet Infrastructure Initiative) workshops around the world, enabling local actors to collaborate on improving the trustworthiness of internet communications through standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF, IPv6, and others. It has become a proven model for raising awareness and stimulating adoption of open, state-of-the-art internet and e-mail security standards and have led to specific actions as a follow-up to the workshops

The workshops follow a **three-module approach**:

1. **Knowledge Transfer** – Explaining standards, their benefits, and regional implementation challenges.
2. **Learning from Practice** – Sharing successful and relevant case studies.
3. **Action Planning** – Jointly defining concrete, region-specific steps to improve deployment.

The GFCE Triple-I model has been widely supported by organizations such as **ICANN, the Internet Society, the Regional Internet Registries (AfriNIC, APNIC, LACNIC, RIPE NCC)**, and various regional IGFs and Schools of Internet Governance. Workshops are often held alongside major regional events (IGFs, RIR meetings, Schools of Internet Governance) to maximize participation and reduce travel costs.

At the core of the model is the "mission": *Enhancing Justified Trust*. Aim is to strengthening user confidence in the internet and e-mail by ensuring access to and use of through secure, state-of-the-art internet standards.

It is key to ensure local ownership. Whereas many of the standards and solutions may be global, in the end it is all about local awareness and implementation. So it is up to local actors to set priorities, ensuring relevance to specific political, economic, and technical contexts.

With the Internet, no one actor can resolve all issues alone. A safe and secure use of the Internet and e-mail depends on all actors in the value chain, thus require inclusive Multi-Stakeholder Engagement. This means that government, private sector, technical community, and civil society need to collaborate on solutions.

Informing local actors with inspirational practices from other places in the world helps – even if thy are not always one-on-one implementable. It is important to learn from real-world deployments, including both successes and lessons learned.

For those who want to create their own workshops the GFCE Triple-I pages offer free resources such as this GFCE Triple-I Handbook and a practical GFCE Triple-I Playbook, based on lessons learned over the years in running GFCE Triple-I meetings around the world. GFCE stands ready to support anyone who wants to deploy such workshops, which will require a modest budget to be available for the specific occasion.

➢ 3.5 Good practice example 5: Coordinated Defense Against DDoS Attacks

Distributed Denial-of-Service (DDoS) attacks have grown in scale, frequency, and sophistication—targeting critical infrastructure, public services, and private enterprises alike. These attacks are often cheap to execute, difficult to attribute, and capable of overwhelming even well-defended systems. Their disruptive impact is no longer limited to IT operations; DDoS now threatens national digital resilience.

Traditional DDoS defenses—such as local filtering, upstream blackholing, or commercial scrubbing services—operate in isolation. This siloed approach creates a systemic vulnerability: defenders only react once under attack, [7][8]while attackers move fluidly across targets. The EU funded CONCORDIA project recognized this fragmentation and proposed a new paradigm: collaborative cyber defense through *Anti-DDoS Coalitions* and a *shared DDoS Clearing House*: "*Today's DDoS threats can only be meaningfully mitigated through early detection, proactive sharing of intelligence, and joint preparedness.*"

3.5.1 Anti-DDoS Coalitions: Trust-Based, Operationally Focused Partnerships

An Anti-DDoS Coalition is a voluntary alliance of trusted actors—ISPs, cloud providers, government agencies, financial institutions, and healthcare operators—that agree to cooperate operationally against DDoS attacks. This coalition model is designed to:

- Accelerate early warning by sharing attack fingerprints in near real time
- Coordinate response through aligned defensive policies and drill-based exercises
- Build mutual trust via clear legal frameworks, NDAs, and defined escalation paths

[7] CONCORDIA project: https://www.concordia-h2020.eu

[8] APNIC Blog on Coalition Model: https://blog.apnic.net/2024/05/14/collaboratively-increasing-the-ddos-resilience-of-digital-societies

The Dutch National Anti-DDoS Coalition[9], coordinated by SURF and SIDN, stands as a leading example. It started as a pilot with a small number of academic and infrastructure providers and now includes over 40 participants. Coalition members meet regularly to share experiences, conduct DDoS simulations, and update governance protocols. Joint drills turned out to be invaluable for building trust and readiness... and for discovering dependencies we hadn't seen before.

3.5.2 The DDoS Clearing House: Shared Situational Awareness

To support this collaboration, CONCORDIA developed the **DDoS Clearing House**, a modular platform enabling the **secure exchange of anonymized DDoS fingerprints**. It comprises three key components:

- **Dissector**: Analyses packet captures or flow logs to generate attack fingerprints in JSON format.
- **DDoS-DB**: A central or federated database storing these fingerprints.
- **Converter**: Translates fingerprints into deployable mitigation rules (e.g. firewall configs, BGP flow specs).

The system is privacy-conscious by design: it does not share payloads or identifiable information, ensuring GDPR compliance while maintaining operational value. Coalition members can use their own dissector tools or the open-source reference implementations provided.

The platform has now moved beyond research and is operational in the Netherlands. Since 2024, the Clearing House[10] has been used in live production settings, enhancing national preparedness and enabling more rapid mitigation of threats. In short: enabling partners to act before the damage is done.

3.5.3 Legal and Governance Frameworks: From Trust to Scale

Collaboration at this level requires not just technical interoperability, but governance and legal alignment. The CONCORDIA team developed practical guides, model NDAs, and operational protocols to support coalition growth. Key lessons include:

- Start with pilot-scale deployments where personal trust exists.
- Establish clear confidentiality, liability, and data use agreements.
- Iterate governance processes as the coalition scales.

[9] NoMoreDDoS technical site: https://www.nomoreddos.org/en/

[10] SIDN Labs on Clearing House: https://www.sidnlabs.nl/en/news-and-blogs/ddos-clearing-house-now-in-use-by-national-anti-ddos-coalition

These practices are now consolidated in the *DDoS Clearing House Cookbook*[11] providing actionable guidance to entities across Europe and beyond.

3.5.4 Conclusion: a blueprint for National and Cross-Border Cooperation

The CONCORDIA project has demonstrated that DDoS resilience is not just a technical issue—it is a collaborative governance challenge. Anti-DDoS Coalitions and the DDoS Clearing House offer a scalable, operationally tested model that complements existing defences and fills the early-warning gap. The CONCORDIA cookbook offers a clear way forward in what is recognized as a real cybersecurity threat – best to be addressed before DDOS attacks target your region, branch or business and learn from practice developed and adopted successfully by those that have been confronted with the challenge already.

➢ 3.6 Good practice example 6: Swiss Banks and Safe Internet Communications

Swiss banks have long been regarded as global leaders in financial discretion and security. As banking has shifted from traditional in-person interactions to digital platforms, Swiss financial institutions have recognized that maintaining trust requires an uncompromising approach to secure Internet communications, and that continued improvement in this will be necessary. The job is never fully done.

3.6.1 Early Adoption: Foundations of Digital Trust

In the early 2000s, Swiss banks were among the first in Europe to implement encrypted online banking portals using HTTPS with strong SSL certificates, ahead of global norms. To mitigate phishing risks and unauthorized transactions, they employed challenge-response mechanisms like TAN lists and hardware tokens.

Recognizing the insecurity of standard e-mail, some institutions introduced encrypted e-mail (PGP/S/MIME), but usability barriers limited widespread adoption. This led to the development of secure internal messaging portals, embedded in authenticated online environments.

3.6.2 Current Best Practices: Multi-Layered, User-Centric Security

Swiss banks operate under the strict oversight of FINMA and adhere to international standards such as ISO/IEC 27001, underpinning a multi-layered approach to digital security. Client communications

[11] https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf

are secured through end-to-end encrypted messaging within web and mobile platforms, while access to digital services is protected by strong multi-factor authentication methods, including photoTAN, QR challenge-response, and hardware tokens. All data in transit is encrypted using TLS, reinforced by certificate pinning, HSTS, and, in some cases, mutual TLS authentication. Mobile banking apps are further hardened with secure enclaves, biometric authentication, and detection mechanisms for compromised devices.

To ensure communication integrity, banks deploy e-mail and domain security standards such as SPF, DKIM, DMARC, DNSSEC, and DANE, minimizing the risk of spoofing and phishing attacks. Internally, institutions are adopting Zero Trust Architecture and micro-segmentation to enforce least-privilege access and reduce exposure in case of intrusion. These defenses are continuously tested through regular security audits, penetration tests, and red teaming exercises.

3.6.3 Next-Generation Secure Networking

These measures can verify and protect clients and servers whilst ensuring financial data that is being transmitted between them cannot easily be read, but does not address all the existing issues with how traffic is actually sent across the Internet.

The Border Gateway Protocol (BGP) has long been the backbone of Internet routing, but was designed in an era when security was not a significant consideration. Whilst security extensions have been developed for BGP such as RPKI and BGPSEC, these are not currently universally deployed and explicit path selection is still not supported.

These concerns led to the Swiss National Bank (SNB) and SIX, the infrastructure provider for around 300 Swiss financial institutions, to adopt the SCION (Scalability, Control and Isolation on Next-Generation Networks) technology when building the Secure Swiss Finance Network (SSFN) in 2021. SCION is a secure, resilient and path-aware routing architecture that allows the Swiss Interbank Clearing (SIC) system that processes around CHF 200 billion interbank and retail payments daily, to operate in a more secure and resilient manner than the previous FinanceIPNet network.

For SSFN, the key benefits are:

- Trust Domains - The use of a trust model based around logical groups of networks sharing a common jurisdiction with agreed trust policies (e.g. SSFN) and a standalone trust root (operated by the voting members SIX, SNB and SWITCH in the case of SSFN) to validate the networks. This ensures that traffic is only exchanged between networks that are members of a trust domain, except that traffic which is explicitly allowed to be exchanged with networks in other trust domains and/or with the rest of the Internet. This also eliminates the possibility of route hijacking and IP address spoofing.

- Path Awareness and Control - The ability to control the paths by which traffic is sent across the Internet. This allows enterprises to explicitly choose and verify the intermediate networks through which traffic is sent, thereby ensuring it does not traverse untrusted networks or through disallowed jurisdictions (e.g. data can remain within Switzerland).
- Resilience & Fast Failover - The ability to switch paths very quickly when connections become congested or fail, which is also beneficial for throttling or blocking malicious traffic. BGP is relatively slow in this respect.
- Multi-ISP Support - The possibility to concurrently use paths provided by different ISPs. This allows commodity Internet connections to be utilised and is more flexible, resilient and cost effective than relying on dedicated point-to-point links or other single ISP solutions. In the event that a single ISP loses all or some connectivity, it is possible to quickly switch to alternative paths using other ISPs.

For Swiss banks and other financial institutions, these requirements were a strong motivation for adopting SCION in an era of growing geopolitical risk, expectations for digital sovereignty, and increased regulatory expectations. The legacy FinanceIPNet was also based on leased lines and MPLS that did not allow for diversity of providers, only offered limited point-to-point rather than multiple connections with single points of failure, and did not have controllable paths offering fast switching in the event of issues. This was inflexible and costly and provided further motivation to adopt SCION.

Looking ahead, Swiss banks are also preparing for the next horizon in security threats, including those posed by quantum computing. It is therefore important to choose technologies that not only have built-in cryptographic agility that allow quantum-safe cryptographic algorithms to be utilised, but which can prevent sensitive data from transversing untrusted and insecure routes. By preventing traffic being collected by unauthorised parties in the first place, there will not be the possibility to decrypt harvested data at some point in the future.

3.6.4 Implementations

Swiss banks make use of SCION that has a commercial implementation developed by **Anapaya** (a commercial spin-off from ETHZ Zurich) who are working with SIX to build and operate SSFN in conjunction with multiple ISPs. Other deployments include the Secure Swiss Healthcare Network (SSHN) for Swiss healthcare providers, the Secure EFTPOS Network (SEPN) for cashless payments, and the Secure Swiss Utilities Network (SSUN) for power utility providers.

There is also an open source implementation developed by the SCION Association that is used for the SCION Education, Research and Academic Infrastructure (SCIERA).

3.4.7 Conclusion

From early adoption of web and e-mail encryption to pioneering the use of SCION-based Internet routing, Swiss banks have consistently placed digital trust and communications security at the core of their digital transformation. Their multi-layered approach - grounded in strong encryption, user-focused design, regulatory alignment, and sovereign networking - offers a model for secure, resilient and future-proof communications in the financial sector and beyond.

4. Comprehensive background of internet standards

In this chapter, a more elaborate description is given of the security-related internet standards that are part of the current scope of Triple-I explained in this document. This description includes the technical workings of the selected standards, the benefits they provide, the adoption challenges and the current adoption status, in relation to Routing Security; DNS Security; and e-mail security.

➢ 4.1 Secure Internet Routing

The global internet depends on the Border Gateway Protocol (BGP) to route traffic between thousands of autonomous systems (ASes) and get packages (IPv4, IPv6) from origin to destination. While BGP has powered the growth of the internet, it was designed without intrinsic security mechanisms. This vulnerability has led to repeated incidents of route hijacking, route leaks, and misconfigurations, disrupting connectivity, enabling surveillance, and exposing users to malicious actors. To address this, a set of technical standards and operational best practices has emerged to secure routing—most notably RPKI, ROA, RPKI-based Route Origin Validation, and most recently also BGPsec. In addition, Internet Society launched the MANRS (Mutually Agreed Norms for Routing Security) community initiative which is today supported by the Global Cyber Alliance, .

In this Chapter we explain the key standards for secure routing, the different stakeholder roles in securing global Internet routing that play a key role in adoption of these standards; the MANRS initiative that supports deployment of these standards and good routing practices in different communities, the current state of maturity in implementation of secure routing practices around the world, and a suggestion for consideration for stakeholders in all regions around the world.

4.1.1. Key Standards for Routing Security

Routing Security is foundational to a stable, trustworthy internet. The following modern internet standards play a key role:

1. RPKI (Resource Public Key Infrastructure): A cryptographically secure framework that allows internet number resource holders to verify which networks are authorized to originate their IP prefixes.
2. ROA (Route Origin Authorization): A digitally signed statement that specifies which AS is allowed to originate a particular IP prefix.

3. RPKI-based Route Origin Validation (ROV): A router feature that classifies BGP route announcements as *Valid*, *Invalid*, or *Unknown* using ROAs, to drop or prefer routes based on origin legitimacy.
4. BGPsec: An emerging BGP extension that cryptographically validates the entire AS path, not just the origin, offering stronger protection against AS path manipulation.

With regards to RPKI (and ROA), ~60% of globally advertised IP address space is covered by ROAs in 2025. Europe leads the way, interest is picking up around the world, and Africa needs to catch up, most.

BGP Origin Validation is enabled on most Tier 1 and Tier 2 networks, and currently ~45% of internet routes are validated at origin. It is widely deployed in the Netherlands, Brazil, Japan, and the U.S. but still needing more attention in upcoming regions.

BGPsec deployment is still in very limited, with pilot deployments only, supported by a few research and government networks. The real-world adoption is still constrained by hardware and performance trade-offs.

4.1.2 Stakeholders Ensuring Routing Security

The Internet functions because of collaboration between many actors. The key actors ensuring routing security include:

- Network Operators (ISPs, IXPs, CDNs): Deploy and maintain ROAs, implement BGP filtering and validation, and commit to MANRS best practices.
- Regional Internet Registries (RIRs): Provide the infrastructure and tools to register ROAs and manage RPKI trust anchors and repositories.
- Governments and Regulators: Increasingly reference or mandate routing security (e.g., U.S. CISA's BGP security initiative; Japan’s MIC encouragement for RPKI adoption; Netherlands PPP Platform Internet Standards’ requirements for “comply or explain” use of RPKI, ROA, etc).
- Standards Bodies (IETF): Develop protocols like BGPsec, RPKI standards, and coordinate improvements to BGP security while ensuring continued interoperability.
- Global Cyber Alliance: Hosts and promotes MANRS, offers guidance, training, and support for global routing security efforts.

4.1.3 Secure routing working practices: MANRS

MANRS stands for *Mutually Agreed Norms for Routing Security*: a global initiative that defines and promotes baseline routing security actions that all network operators should implement to reduce common threats to the internet's routing system. MANRS was launched up by the Internet Society (ISOC), a non-profit organization committed to an open, globally connected, secure, and trustworthy internet, and since 2024 is an activity of the Global Cyber Alliance (GCA), a non-profit organization that works with communities to improve the Internet and help people and organizations be more secure online.

MANRS outlines simple, concrete actions organizations can take, tailored to their role on the Internet, offering four programs for Network Operators, Internet Exchange Points, CDN and Cloud Providers, and Equipment Vendors. Joining MANRS means joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure. Actions in the MANRS programs fall into four main categories:

- Filtering invalid BGP announcements
- Anti-spoofing to stop IP source address falsification
- Coordination among operators to mitigate incidents
- Routing information publication for transparency

MANRS uses a measurement infrastructure to monitor the level of implememtation of the Actions – so-called MANRS readiness scores - by networks all around the globe. The MANRS readiness scores are displayed on the MANRS Website and the MANRS Observatory.

4.1.3 Regional adoption of routing security standards

Making the Internet more robust has become increasingly important for stakeholders around the world as the Internet is becoming more integrated with our lives day by day. The overview below provides an impression of current routing security standards adoption around the world (indicative only, 2025):

- In Europe, RPKI and MANRS are widely adopted, and there are strong policy and technical incentives to stimulate uptake;
- In Latin America, the Regional Internet Registry LACNIC drives awareness. Brazil is a leader in ROA and validation, and MANRS adoption, also through the Secure Internet Brazil program

- North America sees a solid RPKI deployment, yet MANRS participation among smaller ISPs is still limited;
- In the Asia-Pacific we see in particular rapid improvement in Japan, India, and Australia, policy and business driven, yet some of the other countries are still lagging;
- Africa is still in early-stages of RPKI and MANRS implementation efforts; increasing support from ISOC and ICANN;

Notably, MANRS adoption often precedes or complements technical standard uptake, acting as a practical and policy bridge for routing security implementation and doing so by fostering a community that commits to good practice and to evolve the understanding of how good practice looks like.

4.1.4 Emerging Secure Routing Technologies

The Border Gateway Protocol (BGP) is the backbone of Internet routing, but is intrinsically based on unverified trust between networks - namely that a network will only accept traffic destined for its own customers, will only forward traffic to other networks that it can reach, and will not send traffic with fake source IP addresses. BGP also does not provide mechanisms to easily control the path that traffic takes across the Internet, and in particular jurisdictions where sensitive traffic can be intercepted, inspected, subjected to MITM and DoS attacks, or possibly later decrypted.

As mentioned, whilst security extensions have been developed for BGP including RPKI and BGPSEC whilst others such as ASPA (Autonomous System Provider Authorization) and the concept of 'routing zones of trust' have been proposed, none of these can support explicit path selection.

Network operators have tended to utilize other solutions such as MPLS, SD-WAN and Segment Routing which can provide more certainty of path control, but these all have various limitations with respect to support for multiple vendors and across multiple networks. SCION (Scalability, Control and Isolation on Next-Generation Networks) is another secure path-aware routing architecture that has recently been gaining some deployment, although this needs to be specifically supported by border routers.

There is an increasing requirement for path-aware routing even if vendors have yet to converge on a common solution. Nevertheless, it's an issue that is currently being actively discussed at the IETF/IRTF and it's possible that standards will emerge in the next few years.

4.1.5 Conclusion

Routing security is foundational to a stable, trustworthy internet. While technical solutions like RPKI and BGPsec form the cryptographic backbone of secure routing, cooperative frameworks like MANRS ensure operational best practices are followed. MANRS, as an industry-driven and globally supported initiative, bridges the gap between technical standards and real-world deployment by fostering a culture of responsibility and mutual trust.

While new solutions for secure routing are being proposed and developed, one of the main challenge remains with the adoption of these technologies. Slow adoption is aggravated by limited support of these solutions in the network equipment because of the lack of demand, but the real problem is that routing security of a network depends on action of other network operators and requires a concerted action from many networks. This is why efforts like MANRS because they motivate such action.

Another point to note is that there is no one single solution to the routing security problem. One should consider the technologies discussed in this handbook as a toolbox where different components should be applied according to specific circumstances and risk analysis. However, there is a minimum baseline of controls that must be implemented that provide the basis for other solutions. MANRS Actions for its different programs are examples of such baseline.

While adoption of new technologies is getting momentum, the use of traditional best practices is still important. For instance, replying solely on RPKI ROAs in route origin validation may not be sufficient and require a fallback to traditional validation based on the IRR (Internet Routing Registry) system, when needed information in RPKI is not available. Likewise, RPKI does not provide mechanisms for controls of the routing policy, so additional controls based on traditional approaches need to be considered. A good example here is controlling a set of ASNs of the provider "customer cone" that can appear as origins in the customer announcements. RPKI-based technologies currently do not provide mechanisms for that and it need to be complemented by the use of the IRR as-set objects or other means.

The current state of global deployment shows promising momentum, particularly in Europe, Latin America, and advanced networks in Asia and North America, but significant gaps remain, especially in smaller networks and under-resourced regions. Continued awareness-building, supportive regulation, and international cooperation will be essential to achieving full adoption and a secure global routing environment.

4.1.6 Resources on Secure Internet Routing Standards and Practices

1. *Operational Best Practices and Initiatives*

- *Mutually Agreed Norms for Routing Security Initiative (MANRS)*. Available at: https://www.manrs.org
- *MANRS Observatory – Routing Security Monitoring Platform*. Available at: https://observatory.manrs.org

2. *IETF Standards on Routing Security*

- IETF. RFC 6480 – *An Infrastructure to Support Secure Internet Routing*. https://datatracker.ietf.org/doc/html/rfc6480
- IETF. RFC 6482 – *A Profile for Route Origin Authorizations (ROAs)*. https://datatracker.ietf.org/doc/html/rfc6482
- IETF. RFC 6811 – *BGP Prefix Origin Validation*. https://datatracker.ietf.org/doc/html/rfc6811
- IETF. RFC 8205 – *BGPsec Protocol Specification*. https://datatracker.ietf.org/doc/html/rfc8205

3. *Measurement & Deployment Data Sources*

- Center for Applied Internet Data Analysis (CAIDA). *BGPStream and Routing Security Research*. https://www.caida.org
- NLnet Labs. *Routinator and Krill – Open Source RPKI Tools*. Available at: https://nlnetlabs.nl
- RIPE NCC. *RIPEstat Routing Information Portal*. https://stat.ripe.net
- RIPE NCC. *BGPlay – Visual BGP Timeline Viewer*. https://stat.ripe.net/widget/bgplay

4. *Regional Internet Registries (RIRs) – RPKI Support*

- RIPE NCC: https://www.ripe.net/manage-ips-and-asns/resource-management/rpki
- APNIC: https://www.apnic.net/community/security/rpki
- ARIN: https://www.arin.net/resources/manage/rpki/
- LACNIC: https://www.lacnic.net/1080/2/lacnic/rpki
- AFRINIC: https://afrinic.net/support/rpki

5. *Other resources*

- NANOG: *North American Network Operators Group*. https://www.nanog.org
- RIPE Meetings: *RIPE NCC Community Events*. https://www.ripe.net/participate/meetings
- Cybersecurity and Infrastructure Security Agency (CISA). *Protecting Internet Routing Infrastructure*. https://www.cisa.gov

4.2 Secure use of the DNS

The Domain Name System (DNS) is essential to the functioning of the Internet, converting human-readable domain names into IP addresses, yet it remains vulnerable to both technical threats and malicious abuse. DNS abuse, as defined by ICANN, includes malware, botnets, phishing, pharming, and spam when used to support these threats. While technical standards such as DNSSEC and DANE strengthen the security of DNS responses, they must be complemented by proactive abuse prevention and shared operational responsibility across stakeholders.

Unchecked, DNS abuse erodes trust, enables cybercrime, and undermines the stability of the Internet ecosystem. Addressing DNS abuse requires both technical DNS security standards and proactive abuse mitigation measures by actors across the domain name lifecycle.

In this Chapter we outline the importance of DNS security, the key global standards that must be implemented, the stakeholder roles in securing the DNS, and the strategic value of ICANN's KINDNS initiative in promoting operational norms and resilience.

4.2.1 Key Standards for DNS and DNS abuse prevention

A robust DNS security posture is the first line of defense against both technical vulnerabilities and abuse. The following standards are essential:

1. DNSSEC (Domain Name System Security Extensions): Ensures authenticity and integrity of DNS responses using digital signatures to protect against spoofing and pharming, often used in phishing campaigns. In this way it prevents redirection to malicious websites by verifying legitimate domain resolution.
2. DANE (DNS-Based Authentication of Named Entities): Uses DNSSEC to associate domain names with TLS certificates, and thus offers an extra layer of protection for HTTPS and secure e-mail. In this way it helps prevent man-in-the-middle attacks and impersonation in e-mail systems (e.g., phishing).
3. SPF (Sender Policy Framework): DNS-based declaration of authorized mail servers for a domain that detects and blocks spoofed e-mail sources. This is critical to preventing phishing and spam via domain impersonation (see also Chapter 3 E-mail Security: SPF goes hand in hand with DKIM and DMARC).
4. QNAME Minimization (RFC 7816): Reduces unnecessary data disclosure in DNS queries, which enhances user privacy. This limits the amount of information exposed to malicious recursive or authoritative DNS servers.

5. DNS-over-TLS (DoT) / DNS-over-HTTPS (DoH): Encrypt DNS traffic between client and resolver, which prevents eavesdropping and query manipulation. In this way it reduces the risk of DNS hijacking and surveillance, which can be used in targeted abuse.

The Domain Name System Security Extensions (DNSSEC) emerged as a critical response to growing concerns about vulnerabilities in the Domain Name System (DNS), which underpins global internet navigation. DNS, while foundational to internet functionality, was originally designed without security mechanisms, making it susceptible to attacks such as cache poisoning and man-in-the-middle exploits. A milestone was reached in 2010 with the signing of the DNS root zone, enabling a trust anchor. Since then, adoption has grown gradually, driven by security-conscious governments, enterprises, and internet service providers. Key factors supporting deployment include government mandates, growing awareness of DNS threats, and advocacy from initiatives like ICANN’s DNSSEC Deployment Initiative and the Internet Society’s efforts.

However, global adoption remains uneven. While some countries—particularly in Europe and parts of Asia—have high deployment rates, others lag due to lack of awareness, technical complexity, or cost. Registries and DNS operators play a pivotal role, as DNSSEC must be implemented at multiple levels of the DNS hierarchy, including TLDs and domain registrants. As digital trust becomes increasingly important, DNSSEC continues to gain relevance, forming a foundation for broader DNS-based security technologies such as DANE (DNS-based Authentication of Named Entities). Major public resolvers enabled DNNSSEC validation, and more and more top level domains (TLDs) adopted DNSSEC, yet more remains to be done.

DANE/TLSA deployment is still low, with adoption mainly limited to Europe – and mostly used for securing SMTP. SPF is widely deployed due to e-mail service proviers defaults, yet misconfiguration is still high, and today still missing complementary DMARC/DKIM policies see also Chapter on E-mail Security). DoT and DoH deployment is moderate, yet supported by major public resolvers. ISP support and awareness to be grown.

4.3.2 Stakeholders in Ensuring DNS Security and Preventing DNS Abuse

Effectively addressing DNS abuse and security requires a whole-of-ecosystem approach that includes the following key actors:

- Governments: set regulatory requirements for secure domain usage; can mandate DNSSEC for public sector domains; support awareness of DNS abuse and enforcement mechanisms.

- TLD Registries and Operators: enable and promote DNSSEC, support abuse reporting mechanisms, suspend or mitigate malicious domains, and ensure WHOIS accuracy.
- Domain Registrars: provide user-friendly DNSSEC and SPF configuration tools; monitor for abusive registrations; act on abuse complaints quickly.
- ISPs and Resolver Operators: implement DNSSEC validation, DoT/DoH, and anti-abuse filtering; log and report abuse patterns.
- Enterprises and Website Owners: maintain secure DNS configurations; avoid misconfigured SPF/DMARC/DNSSEC that can be exploited; act quickly when domains are abused.
- End Users / Civil Society: demand secure, abuse-resistant infrastructure and report abuse when encountered.
- Abuse Reporting Networks: organizations like APWG, CERTs, and trusted notifier frameworks play a vital role in identifying and mitigating abuse.
- ICANN: hosts and promotes KINDNS, offers guidance, training, and support for DNS security efforts.

Notably, registries and registrars often hold the technical and contractual levers to take down abusive domains, especially when abuse meets ICANN’s definition and contractual enforcement mechanisms apply.

4.2.3 KINDNS: Raising the Bar for Operational Norms and Abuse Prevention, together

To complement protocol-level defenses, KINDNS—Knowledge-Sharing and Instantiating Norms for DNS and Naming Security—provides a voluntary operational framework for DNS operators. Facilitated by ICANN, it encourages adoption of baseline security and abuse mitigation practices by both authoritative and recursive DNS operators.

KINDNS provides a clear, actionable checklist of good practices including DNSSEC validation, rate limiting, incident response, and monitoring. It offers a platform for self-assessment and improvement, and provides guidance that helps operators prevent their infrastructure from being leveraged for abuse (e.g., open resolvers, reflection attacks).

KINDNS supports DNS Abuse Mitigation through encouragement of operators to deploy secure configurations proactively, not just reactively, and through promotion of detection and reporting of abuse-related anomalies. It reinforces the importance of cooperation between registries, registrars, and infrastructure operators in addressing abuse.

KINDNS does not replace contractual obligations or law enforcement as held between ICANN and ICANN's contracted parties (i.e. gTLDs and ICANN accredited registrars), but it raises the operational baseline, reducing the attack surface and increasing resilience across the DNS landscape. Non contracted parties such as ccTLDs can opt in.

4.2.4 Regional state of adoption of DNS security standards

Ensuring justified trust in the use of the Internet requires action, as while the use of the Internet evolves and societies get more dependent on them, the sophistication of abuse rises, too. It is therefore no surprise to see that uptake of modern security standards is more advanced in the regions that embraced the Internet early on – yet the whole world can learn from each other's experiences and actions. The listing below provides an impression of current DNS security adoption around the world (indicative only, status 2025):

- In Western and Northern Europe lead there is high levels of DNSSEC signing and validation; DANE uptake is emerging, especially in DE and NL, but is still in nascent phase. Eastern and Southern Europe show more moderate adoption, with less consistent ISP and registry support.
- In Latin America, DNSSEC signing is low, but resolver validation is growing (~45–55%) in countries like Brazil and Argentina. SPF is common, but DMARC and DANE adoption remain limited across the region.
- In the Caribbean adoption varies widely; most countries show low DNSSEC and security standard uptake. Capacity building and regional collaboration (e.g., via CaribNOG and CTU) are slowly improving awareness.
- In North America Google, Cloudflare, and U.S. government domains require DNSSEC validation; yet signing at the registrant level remains an issue. SPF and DMARC are widely used, while DANE and encrypted DNS are growing slowly.
- In the Asia-Pacific, Japan, Australia, and New Zealand show moderate adoption; others lag due to infrastructure and awareness gaps. Resolver validation is improving, but domain signing and DANE use remain low region-wide. Smaller Pacific islands often rely on public validating resolvers, showing surprising validation rates.
- In Africa, DNSSEC support is available in some ccTLDs but real-world deployment is very limited.
- In the Middle East, some countries support DNSSEC technically, but domain-level signing and validation are rare. Regional collaboration exists, but operational deployment remains limited.

4.2.5 Conclusion

Securing the DNS is no longer a technical luxury—it is a societal necessity. A globally secure DNS ecosystem depends on the alignment of standards, operations, incentives, and accountability. Moving from fragmented best-effort adoption to universal baseline implementation is both achievable and essential for the future stability, trust, and safety of the internet. A secure DNS is the backbone of a secure Internet—and addressing DNS abuse is inseparable from DNS security itself. Global technical standards like DNSSEC, DANE, SPF, and DoH provide critical building blocks. These standards do not stop all abuse at the source, but they make many forms of abuse significantly harder to execute. But it is through operational frameworks like KINDNS and collective responsibility across the stakeholder ecosystem that these tools translate into meaningful protections.

Combined with proactive abuse monitoring and reporting, they create a much safer DNS environment. Proactive DNS security and abuse mitigation are vital to sustaining a trusted and resilient internet infrastructure.

One of the real challenge we are seeing today is the signing at the second level (by registrants). Registrars need more work to make it easy and also enable automation mechanisms for the process to be smooth and reliable.

Key words going forward are awareness raising to all stakeholders affected to ensure the urgency becomes clear, and capacity building and regional support are needed to help lagging regions to come up to speed.

Today, for almost one-third of the world, "getting online" is still the first step to be done. Yet as soon as they are online they are confronted with a world of actors at different levels of sophistication. It awareness raising and capacity building is key to be able to embrace the opportunities while protecting against abuse.

4.2.6 Resources on Secure DNS Standards and Practices

1. Operational Best Practices and Initiatives

- **KINDNS (ICANN Initiative)**
  KINDNS Baseline Practices for Recursive and Authoritative Operators ICANN's initiative promoting operational norms for DNS security and resilience, Availale at https://kindns.org/

- **ICANN DNSSEC and Security Resource Hub**
  Central resources for DNSSEC deployment, DNS Abuse, and resolver hygiene.
  https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en; https://www.icann.org/octo-ssr; https://www.icann.org/dns-security-threats

2. IETF Standards on Secure DNS

- **DNSSEC Core Specifications**
  RFC 4033, 4034, 4035: DNS Security Introduction and Protocols:
  https://datatracker.ietf.org/doc/rfc4033/; https://datatracker.ietf.org/doc/rfc4034/; https://datatracker.ietf.org/doc/rfc4035/

- **DANE (DNS-based Authentication of Named Entities)**
  RFC 6698: The TLSA DNS Resource Record: https://datatracker.ietf.org/doc/rfc6698/

- **SPF (Sender Policy Framework)**
  RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in: E-mail:
  https://datatracker.ietf.org/doc/rfc7208/

- **QNAME Minimization**
  RFC 7816: DNS Query Name Minimisation to Improve Privacy:
  https://datatracker.ietf.org/doc/rfc7816/

- **DNS-over-TLS (DoT):** RFC 7858: Specification for DNS over TLS:
  https://datatracker.ietf.org/doc/rfc7858/

- **DNS-over-HTTPS (DoH):** RFC 8484: DNS Queries over HTTPS:
  https://datatracker.ietf.org/doc/rfc8484/

3. Measurement & Deployment Data Sources

- **APNIC DNSSEC Validation and Deployment Statistics:** Regional and national DNSSEC resolver validation rates and adoption trends: https://stats.labs.apnic.net/dnssec

- **Internet Society Pulse – DNS Security Indicators:** Publicly accessible metrics on DNSSEC deployment and validation by country and region:
  https://pulse.internetsociety.org/security/dns

- **Rick's DNSSEC Root Zone Deployment Tracker:** Status and statistics for TLDs signed with DNSSEC: https://rick.eng.br/dnssecstat/
- **LACNIC DNSSEC Measurement Reports:** Regional analysis of resolver validation and domain signing in Latin America: https://blog.lacnic.net/en/dnssec
- **eco Association – topDNS Initiative:** European benchmark reports on adoption of DNSSEC, SPF, DMARC, and abuse mitigation: https://topdns.eco.de/

4. Abuse Prevention and Reporting

- **ICANN DAAR (Domain Abuse Activity Reporting):** Aggregated abuse data across generic TLDs: https://www.icann.org/octo-ssr/daar
- **NetBeacon (DNS Abuse Reporting Platform)**: Trusted channel for reporting DNS abuse to registrars and registries and ongoing reports tracking trends in DNS abuse globally: https://netbeacon.org/
- **M3AAWG Best Practices for E-mail and DNS Security:** Guidelines for e-mail authentication, DNS hygiene, and abuse response: https://www.m3aawg.org

5. Implementation Guidelines and Toolkits

- **Internet.nl (Test Platform for Internet Standards):** A public tool to test domains and e-mail for compliance with modern internet standards, including DNSSEC, DANE, and TLS: **https://internet.nl/**
- **NLnet Labs DNSSEC How-To (using Unbound, NSD):** https://nlnetlabs.nl/documentation/dnssec/
- **CZ.NIC DNSSEC Practice Statements and Guides (Knot DNS):** https://www.nic.cz/odborne/dnssec/
- **Cloudflare DNSSEC Setup and Validation Tools:** https://developers.cloudflare.com/dns/dnssec/
- **Google Public DNSSEC Implementation and Testing:** https://developers.google.com/speed/public-dns/docs/dnssec

4.3 Securing E-mail: A Global Priority for Digital Trust

E-mail remains the most widely used tool for digital communication across the world—for individuals, businesses, and governments alike. Yet it is also the most exploited vector for cyberattacks. Phishing, spoofing, business e-mail compromise (BEC), and malware delivery continue to result in financial losses, identity theft, and reputational harm. According to the FBI's Internet Crime Report, e-mail-based attacks accounted for billions of dollars in reported losses annually. Beyond financial harm, compromised e-mail systems can jeopardize national security, corporate data integrity, and public trust.

Despite being a decades-old protocol, e-mail was not designed with native security features. Ensuring e-mail security today requires the global deployment of modern authentication, encryption, and policy-based standards. These standards build layered protections that verify the sender, protect message integrity, secure transmission, and enable enforcement actions against fraud and abuse.

In this Section we explain the key standards for e-mail security, the different stakeholder roles in ensuring e-mail security that play a key role in adoption of these standards, the role of DMARC analytic platforms, the current state of maturity in implementation of e-mail security practices around the world, and suggestions for ways forward to enhance justified trust in the use of e-mail.

4.3.1 Key Standards for E-mail Security

Embracing the modern e-mail security standards and policies is the first line of defense against e-mail related threats:

1. SPF (Sender Policy Framework) is a DNS-based e-mail authentication protocol that lets domain owners specify which servers are allowed to send e-mail on their behalf. It validates the sending server against the domain found in the Return-Path (RFC5321.MailFrom) or, if that's missing, the HELO domain. SPF does not validate or protect the "From" (RFC5322.From) address.
2. DKIM (DomainKeys Identified Mail) is an e-mail authentication protocol that uses cryptographic signatures to prove that an e-mail's content and selected headers haven't been modified in transit. The sending server signs the message with a private key, and the recipient verifies it using a public key published in DNS under the domain used in the DKIM-Signature header. DKIM validates the domain that signed the message, not necessarily the one shown in the "From" (RFC5322.From) header..
3. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an e-mail authentication protocol that evaluates the results of SPF and DKIM, and enforces alignment with the domain in the "From" (RFC5322.From) header. For a message to pass DMARC, either SPF or DKIM must both authenticate the message and align with the From domain. If neither does, the receiving server applies the domain owner's policy — none, quarantine, or reject — and, if reporting is enabled, sends aggregate (RUA) and/or failure (RUF) reports to provide visibility into authentication issues and domain abuse..

In addition, MTA-STS (Mail Transfer Agent – Strict Transport Security) and TLS-RPT (TLS Reporting) will help further reduce the risks by ensuring encrypted delivery, and, where feasible, DANE to bind e-mail authentication. The latter is not always possible as DANE authenticates TLS certificates for mail servers via DNSSEC, adding cryptographic trust to server connections, so feasibility depends on DNSSEC availability – and that is still limited despite industry efforts to roll it out more widely.

Furthermore, ARC (Authenticated Received Chain) is a protocol that preserves the original SPF, DKIM, and DMARC results as an e-mail passes through intermediaries like mailing lists or forwarding services. Since forwarding often breaks SPF and can affect DKIM if the message is modified, ARC allows the final recipient to see whether the message was originally authenticated before it was altered in transit. It does this by adding a cryptographically signed chain of headers that records the original authentication state without revalidating it.

BIMI (Brand Indicators for Message Identification) is a visual e-mail standard that allows domains to display their brand logo next to authenticated e-mails in supported inboxes. To qualify, the domain must have a DMARC policy set to quarantine or reject. For full logo display with a blue checkmark, a Verified Mark Certificate (VMC) and a registered trademark are required. Domains without a trademark can use a Certified Mark Certificate (CMC), which enables logo display without the blue checkmark.

E-mail security relies on DNS security DNSSEC (DNS Security Extensions) with regards to DNS integrity, as DNSSEC protects DNS records (including SPF, DKIM, DMARC, DANE) from being forged or altered, which is critical to e-mail trust mechanisms.

4.3.2 Stakeholders Ensuring E-mail Security

The deployment and proper configuration of e-mail security standards rely on coordination among multiple actors:

- Domain Owners (e.g. businesses, governments, NGOs): Must publish accurate SPF, DKIM, and DMARC records and enforce strong policies.
- E-mail Service Providers (ESPs) must support DKIM signing, TLS/MTA-STS for secure transmission, and provide customers with the ability to configure custom DKIM domains to ensure alignment with their From address. Support for SPF alignment should also be available when applicable.

- Registries and Registrars: Can promote default security configurations and raise awareness among domain buyers.
- Network Operators and ISPs: Play a role in supporting DNSSEC and secure e-mail routing.
- Governments and Regulators: Can encourage or mandate adoption of e-mail authentication standards in public and critical infrastructure domains.
- DMARC Analytics Platforms: Help organizations interpret DMARC reports, configure records correctly, and monitor abuse—accelerating secure deployment and reducing complexity.
- End Users and Organizations: Should use e-mail clients that validate security indicators and be trained to recognize suspicious communications.
- Security Researchers and NGOs: Organizations like NetBeacon and Internet.nl help improve abuse reporting and configuration testing across the ecosystem.

4.3.3 DMARC: Cornerstone of E-mail Domain Protection

At the heart of e-mail security lies DMARC—a protocol that connects and enforces the outcomes of SPF and DKIM. It is the first widely adopted standard that empowers domain owners to explicitly declare how their domain should be handled if unauthenticated e-mails are received. This is crucial in stopping phishing e-mails that appear to come from trusted domains.

By enforcing a DMARC policy, domain owners can instruct recipient mail servers to either reject, quarantine, or monitor unauthorized e-mails. Moreover, DMARC provides reporting mechanisms that offer insight into who is using (or abusing) a domain for e-mail. This visibility not only helps stop spoofing but also provides valuable data to improve security posture.

Importantly, DMARC has broader economic and societal value: when widely deployed, it protects brand reputation, secures user trust, and significantly reduces the volume of fraudulent and malicious e-mail traffic on the internet. Adoption of DMARC—particularly with a reject policy—is considered a baseline for trustworthy digital communications.

Implementing DMARC can be approached incrementally to minimize disruption while maximizing protection. Domain owners should start by publishing a DMARC record with a "none" policy (p=none) to monitor e-mail flows without affecting delivery. This enables the collection of DMARC reports from recipient mail servers, which can be analysed—either manually or through tools and services—to identify legitimate sources and unauthorized uses of the domain. Once confident that all authorized e-mail sources are properly configured with SPF and DKIM, the policy can be gradually tightened to "quarantine" and eventually "reject" unauthenticated messages.

E-mail service providers and IT administrators can streamline this process by using DMARC analytics platforms like EasyDMARC, Valimail, or dmarcian, which simplify reporting, configuration checks, and policy management. Clear documentation, testing tools such as Internet.nl, and public support resources from organizations like ICANN, the Internet Society, and NetBeacon further facilitate adoption across sectors.

4.3.4 Regional Adoption of E-mail Security Standards and Practices

Progress on the adoption of e-mail security standards in a region is largely determined by a combination of regulatory mandates, technical capacity, awareness, and infrastructure maturity.

Regions with strong cybersecurity policies, such as government requirements for DMARC or TLS enforcement, tend to see faster and broader uptake, especially when combined with national CERT support and capacity-building programs. The presence of technical expertise within ISPs, IT administrators, and public sector agencies is critical for correct implementation and maintenance of standards like SPF, DKIM, and DMARC. Moreover, access to monitoring and analytics tools, regional collaboration (e.g. through RIRs and multistakeholder initiatives), and the prioritization of digital trust and anti-abuse measures within digital transformation strategies play a key role in sustaining adoption momentum.

The listing below provides an impression of current e-mail security standards adoption around the world (indicative only, situation in 2025):

- Europe shows strong and growing adoption of e-mail security standards, driven by stringent data protection regulations (e.g. GDPR) and widespread digital governance frameworks. SPF and DKIM are well-deployed across government and enterprise domains, while DMARC adoption—especially with a “reject” policy—is increasingly promoted by national cybersecurity agencies (e.g. NCSC-NL, ANSSI, BSI). Countries like the Netherlands, Norway, and the UK are considered regional leaders in deploying DMARC with enforcement.
- Latin America adoption is uneven. Larger economies like Brazil, Mexico, and Argentina are improving SPF and DKIM deployment, but DMARC uptake remains moderate, especially among public sector domains. Regional organizations like LACNIC and NIC.br are working to raise awareness, and some governments have begun mandating DMARC for critical infrastructure. Technical capacity and resource gaps remain challenges in several countries.

- Caribbean shows relatively low adoption rates of SPF, DKIM, and DMARC, though there are exceptions in more digitally advanced territories (e.g. Jamaica, Trinidad & Tobago). Regional collaboration through organizations like CTU (Caribbean Telecommunications Union) and OAS-CICTE is fostering capacity-building efforts to improve cyber hygiene, including e-mail authentication.
- North America leads globally in adoption of e-mail security standards. In the United States, the federal government mandates DMARC implementation across executive branch domains (BOD 18-01), and enforcement rates are high. Major tech companies and financial institutions widely adopt SPF, DKIM, and DMARC with strong enforcement. Canada also demonstrates strong uptake, with support from its Centre for Cyber Security and active industry participation.
- Asia-Pacific presents a mixed landscape. Economies like Japan, Australia, Singapore, and South Korea show high adoption of SPF and DKIM, with increasing DMARC use—often led by financial, telecom, and government sectors, and also DMARC uptake is high in Australia and New Zealand. However, in South and Southeast Asia, adoption is more limited, especially in smaller enterprises and public institutions. Pacific island nations lag behind due to resource limitations but are increasingly supported through regional cybersecurity and digital transformation initiatives. Regional cooperation via APTLD, APNIC, and CERTs helps foster best practices.
- Africa faces significant challenges in e-mail security adoption due to limited technical capacity and infrastructure. While SPF deployment is relatively common among larger organizations, DKIM and DMARC remain underused, particularly in government and education sectors. Initiatives by AFRINIC, regional CERTs, and awareness campaigns by organizations like ISOC and the GFCE are gradually increasing understanding and uptake.

Within Africa, Sub-Saharan regions often show the lowest adoption rates. Few government domains have implemented DMARC with enforcement, and technical expertise is still developing. Nigeria and South Africa stand out with higher deployment and national-level engagement. Targeted training and inclusion in capacity-building partnerships remain key to progress.

The Middle East exhibits varying adoption. The Gulf Cooperation Council (GCC) states, particularly the UAE and Saudi Arabia, have made progress in SPF and DKIM deployment in government and banking sectors, with growing DMARC uptake. However, in broader civil and private sectors, adoption lags. Geopolitical fragmentation and infrastructure gaps pose challenges for unified progress.

4.3.5 Conclusion on e-mail security

Despite being a foundational layer of global digital communication, e-mail remains a persistent weak point in cybersecurity. While standards such as SPF, DKIM, and DMARC have proven effective in reducing spoofing, phishing, and business e-mail compromise, their global adoption is uneven and often incomplete. Many domains still lack proper configurations or fail to enforce strict policies like DMARC "reject," leaving users vulnerable to impersonation attacks. Encryption and transport-layer security measures like MTA-STS and DANE also remain underutilized, particularly outside of digitally mature regions. Without full implementation and monitoring, these standards cannot deliver their intended protection.

To improve the current state, governments, large platforms, and service providers must lead by example, adopting and enforcing e-mail authentication standards across all domains under their control. Regulatory encouragement or mandates, as seen in the U.S. and parts of Europe, are effective levers for accelerating adoption. At the same time, DMARC analytics platforms such as EasyDMARC, Valimail, dmarcian, and Proofpoint can significantly simplify the implementation process. These platforms provide actionable insights from DMARC and TLS-RPT reports, highlight misconfigurations, detect unauthorized use of domains, and support the step-by-step transition from monitoring to enforcement policies. By reducing technical complexity, these tools make e-mail security more accessible to organizations of all sizes and technical capacities.

Improving global e-mail security matters not only for reducing the volume and impact of cybercrime but also for **reinforcing digital trust**, which underpins modern economies, governance, and social interaction. When e-mail cannot be trusted, the broader digital environment becomes fragile—undermining user confidence, disrupting services, and enabling fraud at scale. A secure, authenticated, and encrypted e-mail ecosystem is therefore not just a technical objective, but a **strategic requirement for resilient digital societies**. Public-private collaboration, enhanced tooling, and targeted policy actions can close the gap between available standards and actual protection—strengthening the security and integrity of global communications.

4.3.6 Resources on Secure e-mail Standards and Practices

1. Technical Standards and Specifications (IETF)

- **SPF** – *RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-mail. Available at* https://datatracker.ietf.org/doc/html/rfc7208
- **DKIM** – *RFC 6376: DomainKeys Identified Mail (DKIM) Signatures. Available at* https://datatracker.ietf.org/doc/html/rfc6376
- **DMARC** – *RFC 7489: Domain-based Message Authentication, Reporting & Conformance. Available at* https://datatracker.ietf.org/doc/html/rfc7489
- **ARC** – *RFC 8617: The Authenticated Received Chain (ARC) Protocol. Available at* https://datatracker.ietf.org/doc/html/rfc8617
- **MTA-STS** – *RFC 8461: SMTP MTA Strict Transport Security (MTA-STS). Available at* https://datatracker.ietf.org/doc/html/rfc8461
- **TLS Reporting** – *RFC 8460: SMTP TLS Reporting (TLS-RPT). Available at* https://datatracker.ietf.org/doc/html/rfc8460
- **DANE for SMTP** – *RFC 7672: DANE SMTP Security via TLSA Records. Available at* https://datatracker.ietf.org/doc/html/rfc7672
- **DNSSEC** – *RFC 4033, 4034, 4035: DNS Security Extensions. Available at* https://datatracker.ietf.org/doc/html/rfc4033

2. Best Practice Initiatives and Guides

- **KINDNS (Knowledge-sharing and Instantiation of DNS Security Best Practices)** – Initiative by ICANN. Available at https://kindns.org
- **Internet Society: Deploy360 – E-mail Authentication Deployment.** Available at https://www.internetsociety.org/deploy360/e-mail/
- **Global Forum on Cyber Expertise (GFCE): Triple I – E-mail Security Guidance.** Available at https://thegfce.org
- **M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group)** – Best Practices for senders, receivers, and domain owners. Available at https://www.m3aawg.org/published-documents
- **NCSC (UK) E-mail Security Guidance** – Government-level deployment recommendations. Available at https://www.ncsc.gov.uk/guidance/e-mail-security-and-anti-spoofing

3. Monitoring, Testing & Abuse Reporting Tools

- **Internet.nl** – Comprehensive testing tool for e-mail security standards. Available at https://internet.nl
- **NetBeacon.org** – Central platform for reporting and acting on e-mail abuse (phishing/spam). Available at https://netbeacon.org
- **Internet Society Pulse: E-mail Security Metrics Dashboard.** Available at https://pulse.internetsociety.org
- **EasyDMARC –** DMARC report analysis, SPF/DKIM record validation, automated suggestions. Available at https://easydmarc.com
- **DMARC.org** – Information and resources on DMARC deployment and impact. Available at https://dmarc.org

5. Additional resources

Please find below a number of resources that may be useful when considering action in your region. Please note that whereas your region may have a different deployment situation and regulatory scheme you may still learn from what worked elsewhere – learning together is at the core of advancing together towards increasing justified trust in the use of the internet and e-mail in your region:

➢ IPv6 Deployment & Adoption

- **APNIC. (2021, February). *IPv6 in 2020*:** Regional analysis of IPv6 user growth trends and the pandemic's impact on adoption. https://labs.apnic.net/presentations/store/2021-03-02-ipv6-deployment-status-apnic51.pdf
- **Huston, G. (2021, February). *An IPv6 update for 2020*.**Commentary on major IPv6 deployments by large ISPs and countries. https://www.potaroo.net/ispcol/2021-02/ipv62020.pdf
- **IETF. (2024). *RFC 9386 – IPv6 Deployment Status*.** Comprehensive survey of IPv6 adoption across sectors and geographies. https://datatracker.ietf.org/doc/rfc9386/
- **Wikipedia. (2025). *IPv6 deployment*.** Current global and country-level IPv6 adoption statistics and trends. Retrieved August 14 2025, from https://en.wikipedia.org/wiki/IPv6_deployment

➢ DNSSEC Deployment, Security & Abuse Mitigation

- **APNIC. (2023, September 18). *Measuring the use of DNSSEC*.** Comparative statistics on DNSSEC-enabled domains across ccTLDs. https://blog.apnic.net/2023/09/18/measuring-the-use-of-dnssec/
- **Engelbrecht, R. (2025). *DNSSEC deployment dashboard*.** Live statistics on DNSSEC-signed TLDs and recent root zone changes. https://rick.eng.br/dnssecstat/
- **Heftrig, E., et al. (2024, June). *KeyTrap: DNSSEC algorithmic complexity attack*.** Academic disclosure of a severe DNSSEC-related DoS vulnerability. https://arxiv.org/abs/2406.03133
- **ICANN. (2024, May 23). *Root zone algorithm rollover study*.** Technical review and recommendations for DNSSEC algorithm changes at root level. https://www.icann.org/en/system/files/files/root-zone-algorithm-rollover-study-23may24-en.pdf

- **Recorded Future. (2024). *DNSSEC deployment landscape*.** Data-driven view of DNSSEC penetration by domain type and provider. https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/dnssec

- **UpGuard. (2025, July). *DNSSEC and cybersecurity risk*.** Explains the role of DNSSEC in preventing spoofing and mitigating DNS abuse. https://www.upguard.com/blog/dnssec-risk

➢ E-mail Authentication & Security

- **Google. (2024, October). *Bulk sender guidelines*.** New Gmail requirements for SPF, DKIM, and DMARC for high-volume senders. https://workspace.google.com/blog/product-announcements/gmail-new-e-mail-sender-requirements

- **Yahoo. (2024, October). *E-mail sender best practices*.** Mandatory authentication standards for deliverability to Yahoo Mail. https://senders.yahooinc.com/bulksenderguidelines

- **UK National Cyber Security Centre. (2024). *Mail Check service*.** Government service for monitoring SPF, DKIM, and DMARC compliance. https://www.ncsc.gov.uk/information/mail-check

- **EasyDMARC. (2025, April 25). *E-mail security protocols and why they're important*.** Explains how EasyDMARC simplifies deployment of SPF, DKIM, DMARC, MTA-STS, TLS-RPT, and BIMI. https://easydmarc.com/blog/e-mail-security-protocols-and-why-theyre-important

- **EasyDMARC. (2025, July 10). *National DMARC enforcement: How government action influences e-mail security*.** Evidence of how national policy mandates dramatically improve DMARC adoption and reduce phishing. https://easydmarc.com/blog/national-dmarc-enforcement-how-government-action-influences-e-mail-security

➢ Routing Security

- **Internet Society. (2022). *MANRS 2022 progress report*.** Global status of Mutually Agreed Norms for Routing Security implementation.https://www.manrs.org/2022/11/manrs-2022-progress-report

- **ICANN Office of the CTO. (2023). *Routing security: RPKI deployment status*.** Analysis of global RPKI adoption rates and impact on route hijack prevention. https://www.icann.org/octo-technical-reports

- **GCA. (2022, May 5). *Routing Security Survey Report: Findings III*.** Insights into operational efforts by network operators—including RPKI, IRR and defensive filtering. https://globalcyberalliance.org/routing-security-survey-report-findings-iii/
- **Mirdita, D., Schulmann, H., & Waidner, M. (2024, August). *SoK: An Introspective Analysis of RPKI Security*.** Systematic study revealing that nearly half of global RPKI validators suffer from vulnerabilities or misconfigurations—key for assessing practical security risks. https://arxiv.org/abs/2408.12359
- **Schulmann, H., Vogel, N., & Waidner, M. (2024, September). *RPKI: Not Perfect But Good Enough*.** Comprehensive assessment of current RPKI deployments, noting resilience, security risks, and alignment with U.S. federal expectations (White House roadmap).https://arxiv.org/abs/2409.14518
- **Comms-SCC. (2025, June 2). *Deploying Resource Public Key Infrastructure (RPKI): Steps for Prioritization and Implementation*.** Consensus guidance following the U.S. White House routing security roadmap—helps operators understand risks and how to deploy RPKI effectively. https://www.comms-scc.org/2025/06/02/deploying-resource-public-key-infrastructure-rpki-steps-for-prioritization-and-implementation/
- **Cloudflare. (2024, September 2). *Making progress on routing security: the new White House roadmap*.** Overview of U.S. federal recommendations for BGP security (ROA issuance, RPKI adoption, risk plans), and adoption metrics (e.g., 53% of IPv4 prefixes signed). https://blog.cloudflare.com/white-house-routing-security/
- **Federal Register. (2024, June 17). *Reporting on Border Gateway Protocol Risk Mitigation: Progress & Secure Internet Routing*.** Proposed rule requiring service providers to file BGP routing security risk management plans and document RPKI adoption. https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

➢ Relevant Regulatory & Policy Updates

- **European Commission. (2022). *Study on DNS abuse*.** Policy recommendations for detecting and mitigating DNS abuse in the EU. https://op.europa.eu/en/publication-detail/-/publication/f1eb6f9d-fb2f-11ec-b939-01aa75ed71a1
- **European Commission. (2023). *DNS4EU project overview*.** EU-funded initiative to deploy a protective DNS resolver for public services. https://ec.europa.eu/digital-strategy/our-policies/dns4eu

- **European Commission. (2024, October 17). *Commission Implementing Regulation (EU) C(2024) 7151*.** Sets technical and methodological requirements under the NIS2 Directive, including for DNS operators. https://ec.europa.eu/newsroom/dae/items/819094
- **European Union. (2022). *Directive (EU) 2022/2555 (NIS2 Directive)*.** Establishes EU-wide cybersecurity obligations, including for DNS operators. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
- **ICANN. (2024, February 5). *DNS abuse contractual amendments*.** Updates gTLD registry/registrar contracts to strengthen DNS abuse mitigation. https://www.icann.org/resources/pages/dns-abuse-amendments-2024-02-05-en

National Rollout Plans & Mandates

- **Government of India. (2025, August). *National Broadband Mission 2.0*.** National digital infrastructure roadmap including IPv6 adoption targets. https://dot.gov.in
- **Ministry of Industry and Information Technology of the People's Republic of China. (2021, November). *Notice on accelerating and deeply promoting IPv6 deployment*.** National action plan with 2025 IPv6 usage and IPv6-only transition goals. http://www.miit.gov.cn/
- **Netherlands Government. (2023, July 1). *Besluit digitale overheid*.** Legal requirement for HTTPS, HSTS, and adoption of secure internet standards in government IT. https://wetten.overheid.nl
- **United States Office of Management and Budget. (2020, November 19). *M-21-07: Completing the transition to IPv6*.** Mandates ≥ 80% IPv6-only federal assets by FY2025. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf
- **United States Office of Management and Budget. (2022, January 26). *M-22-09: Moving the U.S. Government toward Zero Trust Cybersecurity Principles*.** Embeds IPv6 adoption into a broader federal zero-trust strategy. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
- **UK Government Digital Service & NCSC. (2023). *Government e-mail security standards*.** Mandates SPF, DKIM, and DMARC for all government domains. https://www.ncsc.gov.uk/collection/e-mail-security
- **Viet Nam Ministry of Information and Communications. (2021). *IPv6 for Government and national targets 2021–2025*.** National plan aiming 100% IPv6 adoption for all internet subscribers by 2025. https://vnnic.vn

- **Communications, Space & Technology Commission (Saudi Arabia). (2023). *Internet indicators and IPv6 adoption report*.** Annual IPv6 adoption tracking and policy guidance for Saudi operators. https://www.cst.gov.sa

The first version of this document was drafted and developed in cooperation with TNO for the Global Conference on Cyberspace GCCS in India (2017). Since, the document has been updated several times in interaction with the global Internet community, and we thanks the following organizations for their contributions to the substantive 2025 update: ICANN, Internet Society, Global Cyber Alliance, RIPE NCC, APNIC, LACNIC, AFRINIC, SCION Association, EasyDMARC, Dutch Platform Internet Standards, M3AAWG, and all participants to the GFCE Triple-I events around the world. Many thanks to all that contributed.

Contact Us

For more information about the GFCE or the Triple-I initiative, please reach out to the GFCE Secretariat at **contact@thegfce.org**

To stay updated about the GFCE projects, activities and initiatives, check out our website and follow us on our social media channels.

thegfce.org @thegfce