

Procuring Modern Security Standards by Governements and Industry

Speakers and panel members



Olaf Kolkman: Internet Society, moderator



Satish Babu, ICFOSS, SIFFS, ISOC, ICANN CSI



Flavio Kenji Yanai, NIC Brasi, software engineer



Mallory Knodel: Center for Democracy & Technology and Internet Architecture Board (IETF),



Wout de Natris: Coordinator IGF Dynamic Coalition Internet Standards, Security and Safety Coalition (IS3C)



Gerben Klein Baltink, voorzitter Platform Internet Standaarden



Annemieke Toersen: advisor of Netherlands Standardization Forum



Gilberto Zorello, NIC Brasil, project responsible for coordinating the Program for a safer Internet

Olaf Kolkman

- Internet Society (ISOC) Principal – Internet Technology, Policy and Advocacy
- IETF
- Council Bits of Freedom; Global Partners Digital
- GFCE, GCSC, DNSSEC - IANA



Programme – part 1

Introduction
by Olaf Kolkman

13:30 – 13:40

Procurement and Supply Chain Management
and the Business Case, by Wout de Natris

13:55 – 14:15

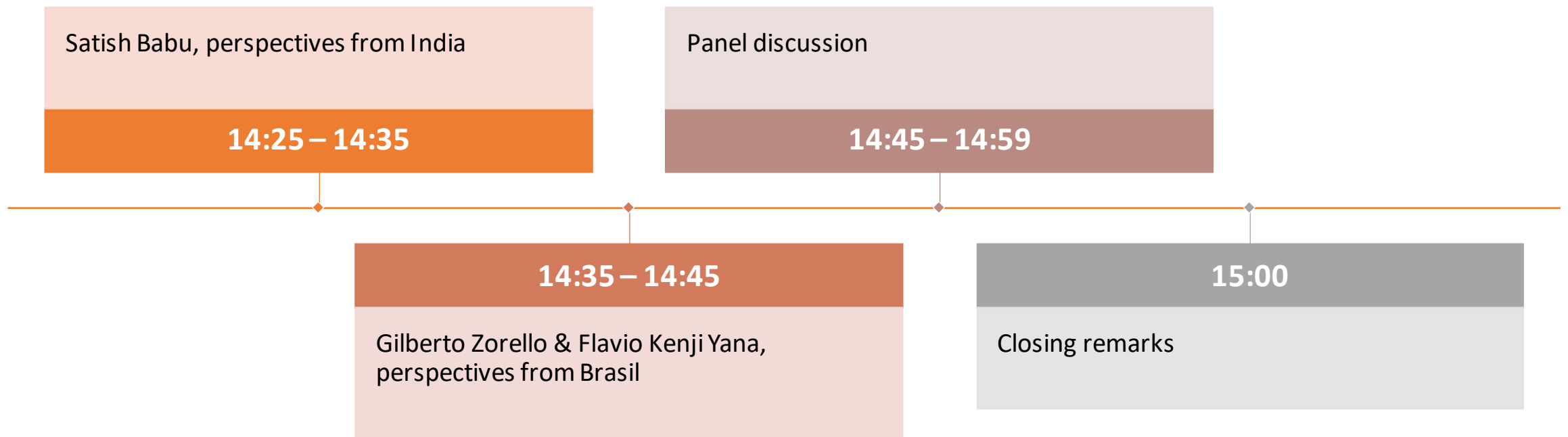
13:40 – 13:55

the Role of Open Standards particularly in
procurement, experiences in the Netherlands,
by Gerben Klein Baltink & Annemieke Toersen

14:15 – 14:25

Questions in the audience

Programme – part 2





Gerben Klein Baltink

- Platform Internet Standards in the Netherlands
- Adoption
- Tooling



12th October 2023

Procuring modern security
standards by
governments&industry

**Forum
Standaardisatie**

Standaard Samenwerken

Annemieke Toersen
Netherlands Standardisation Forum

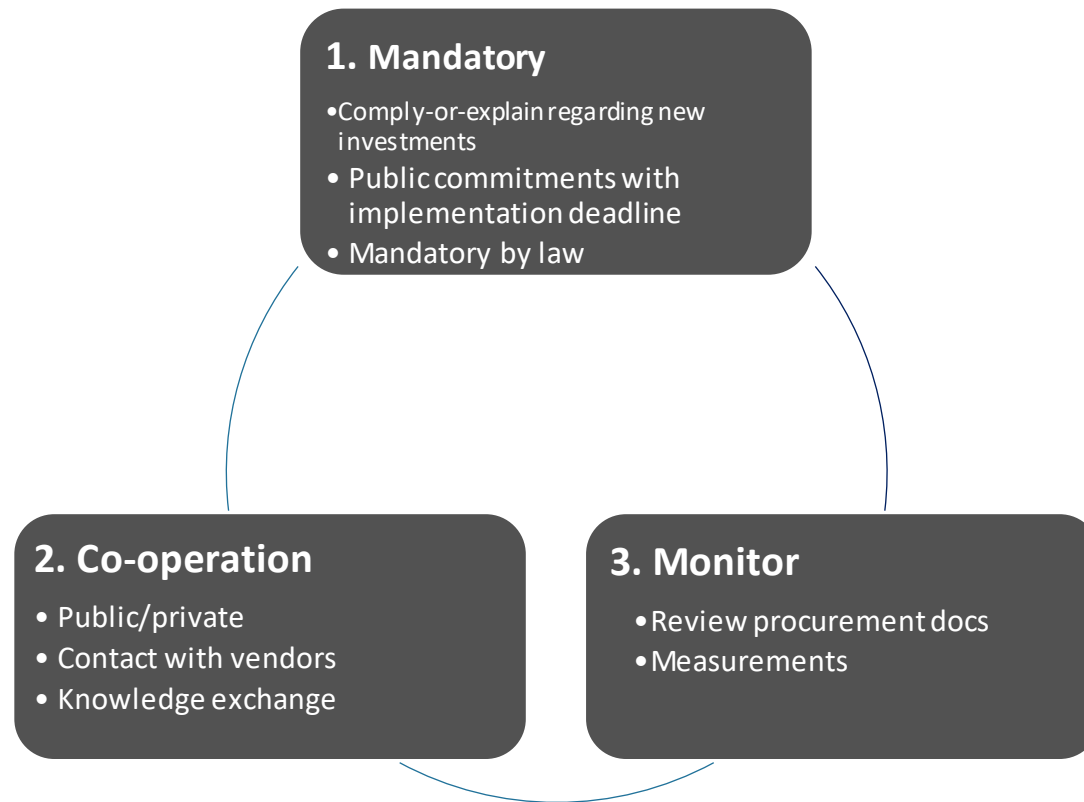
Netherlands Standardisation Forum

- Thinktank on interoperability that advises Dutch government
- Members from government, businesses and science
- List with mandatory open standards
- Scope: public sector organisations

Why open standards?

- Interoperability
- Security
- Accessibility
- Vendor neutrality

Adoption strategy internet security standards



Internet standards and market failure

1. **Network effects**

- “First user disadvantage...” → critical mass is needed

2. **Information asymmetry**

- “End users don’t know and can’t verify...” →
more transparency and awareness is needed

- Study “Economic aspects of Internet security” by Netherlands Bureau for Economic Policy Analysis, <https://www.cpb.nl/sites/default/files/publicaties/download/ad-kox-straathof-economic-aspects-internet-security.pdf>

1. Mandatory: comply-or-explain

- List with over 40 open standards;
- Evaluated against criteria (“openness”, “added value”, “market support” and “proportionality”).)
- Different categories (internet and security, document and web, e-invoicing and administration etc.)
- When governments invest/procure they must choose for the relevant standards on the list;
- Governments may only deviate when there is a severe reason (like extreme costs), and they should report on the deviation in their annual report.



What modern internet security standards?

- DNSSEC (signed domain)
- HTTPS+HSTS (secure website connection)
- DMARC+DKIM+SPF (prevention of mail spoofing)
- STARTTLS+DANE (prevention of mail eavesdropping)
- RPKI (authorised internet routing)
- security.txt (contact information for vulnerability disclosure)
- IPv6 (modern internet address)
- Others: SAML, OpenID Connect, STIX/TAXII

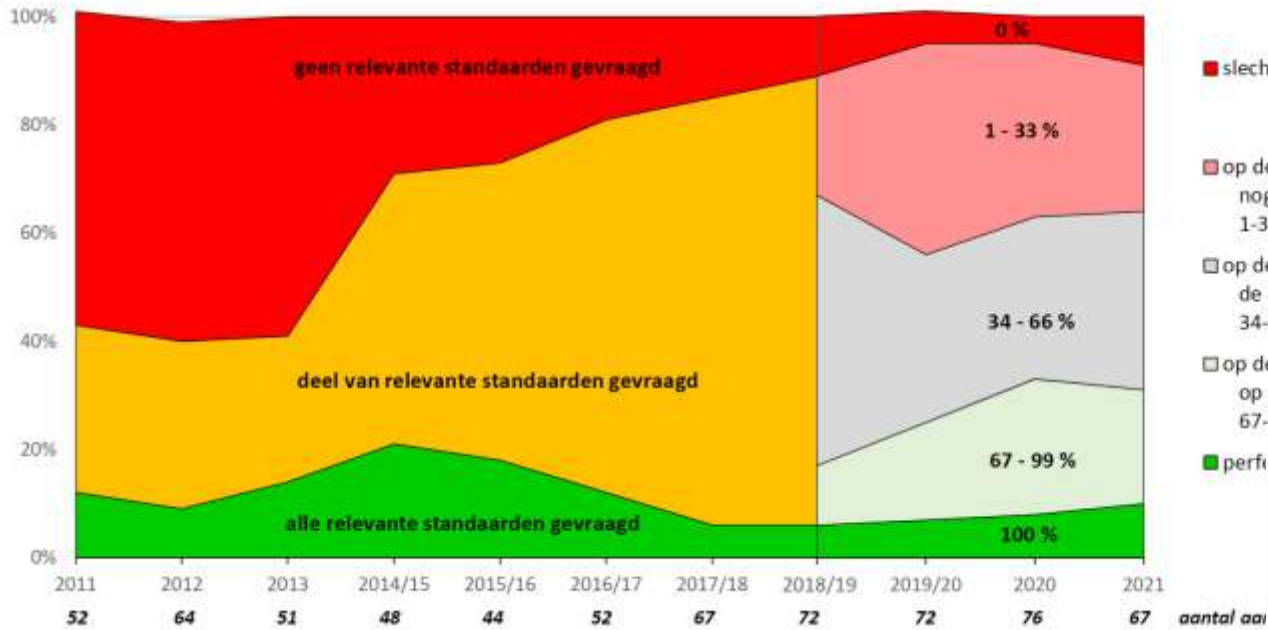
2. Co-operation (including contacts with vendors)

- National: Internet Standards Platform, Secure Mail Coalition
- International:
 - MESSEU (workshops Modern Email Security Standards EU governments)
 - Reuse of Internet.nl code: aucheck.com.au (Australia), top.nic.br (Brazil), sikkerpaa nettet.dk (Denmark)
- Contact with vendors and hosters like Cisco, Microsoft, OpenExchange, Google, Akamai, Cloudflare, Mijndomein, One.com and Your.online.



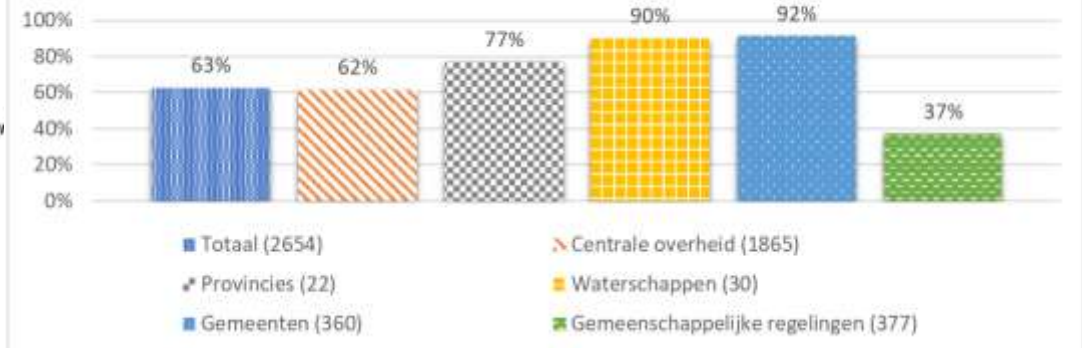
3. Monitoring (also procurement documentation)

'Pas toe' bij aanbestedingen

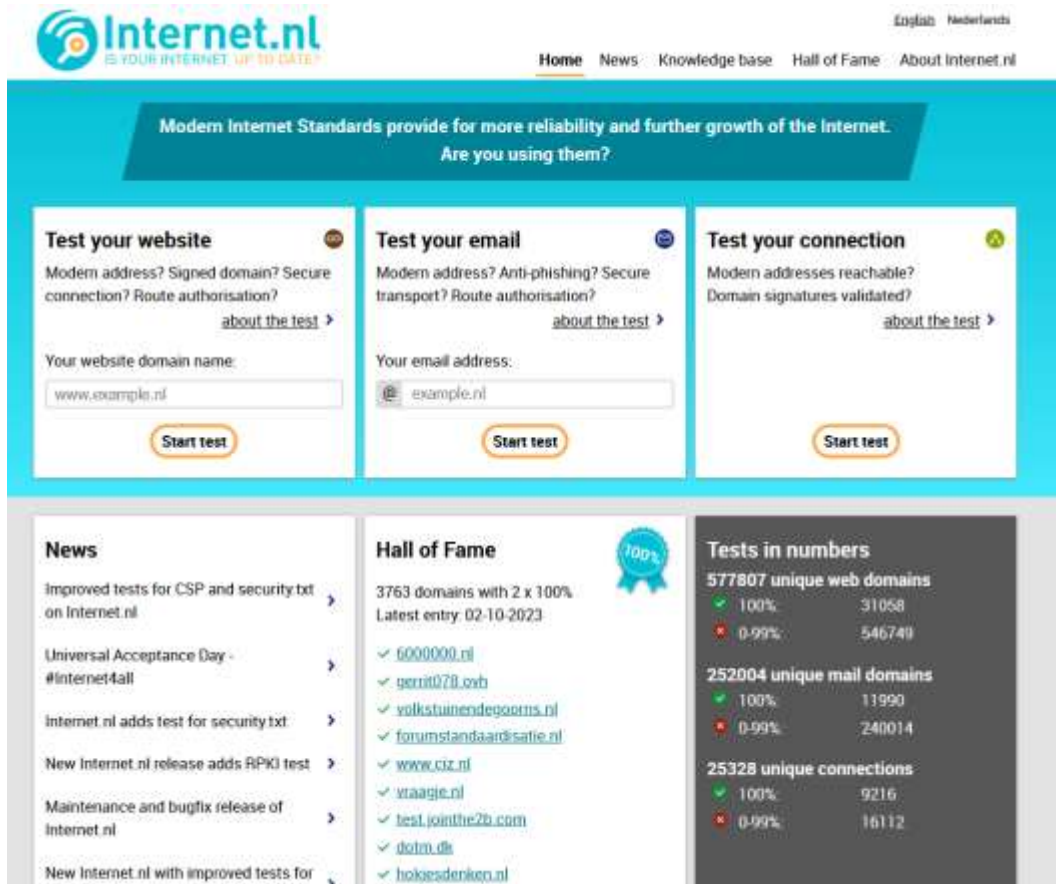


- slecht: 0%
- op de goede weg / nog een heel eind te gaan: 1-33% gevraagd
- op de goede weg / de middenmoot: 34-66% gevraagd
- op de goede weg / op weg naar perfect: 67-99% gevraagd
- perfect: 100%

% volledige adoptie webbeveiligingsstandaarden per overheidscategorie



3. Monitoring using Internet.nl



Internet.nl
IS YOUR INTERNET UP TO DATE?

English Nederlands

Home News Knowledge base Hall of Fame About Internet.nl

Modern Internet Standards provide for more reliability and further growth of the Internet. Are you using them?

Test your website

Modern address? Signed domain? Secure connection? Route authorisation?

[about the test >](#)

Your website domain name:

Start test

Test your email

Modern address? Anti-phishing? Secure transport? Route authorisation?

[about the test >](#)

Your email address:

Start test

Test your connection

Modern addresses reachable? Domain signatures validated?

[about the test >](#)

Start test

News

- Improved tests for CSP and security.txt on Internet.nl >
- Universal Acceptance Day - #Internet4all >
- Internet.nl adds test for security.txt >
- New Internet.nl release adds RPki test >
- Maintenance and bugfix release of Internet.nl >
- New Internet.nl with improved tests for >

Hall of Fame

3763 domains with 2 x 100%
Latest entry: 02-10-2023

- 6000000.nl
- gerit078.ovb
- volkstuiendegeocoms.nl
- forumstandaardsatie.nl
- www.ciz.nl
- vraagje.nl
- test.jointhe2b.com
- doin.de
- hokgesdenken.nl

Tests in numbers

577807 unique web domains

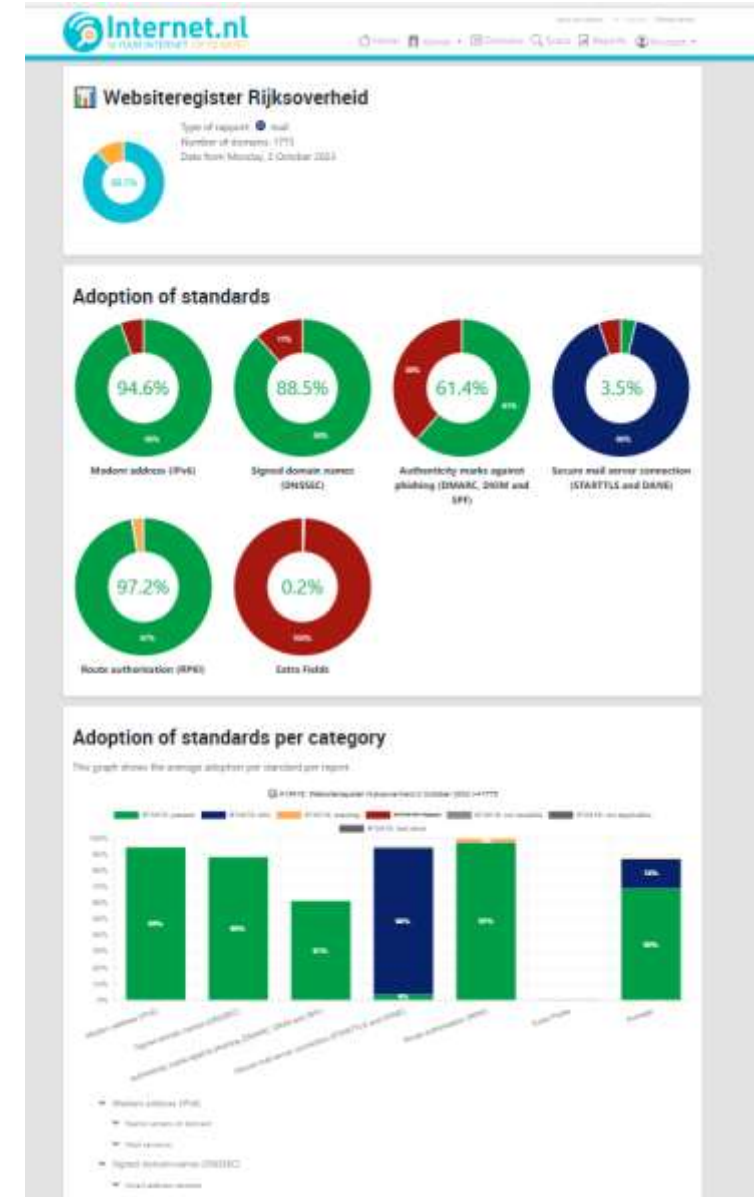
- 100%: 31058
- 0-99%: 546749

252004 unique mail domains

- 100%: 13990
- 0-99%: 240014

25328 unique connections

- 100%: 9216
- 0-99%: 16112



Internet.nl

Websiteregister Rijksoverheid

Type of support: mail
Number of domains: 1771
Data from: Monday, 2 October 2023

Adoption of standards

- Modern address (IPv6): 94.6%
- Signed domain names (DNSSEC): 88.5%
- Authenticity marks against phishing (DMARC, DKIM and SPF): 61.4%
- Secure mail server connection (STARTTLS and DANE): 3.5%
- Route authorisation (RPki): 97.2%
- Extra fields: 0.2%

Adoption of standards per category

This graph shows the average adoption per standard per report.

Legend: IPv6 address, Signed domain names, Authenticity marks, Secure mail server connection, Route authorisation, Extra fields.

**If you don't ask it...
You don't get it.**



Questions?

- More info:
- <https://www.forumstandaardisatie.nl>
- <https://internet.nl/>





**MAKING THE INTERNET
MORE SECURE AND SAFER**

IS3C
Internet Governance Forum
Open Forum #57
Kyoto, Thursday 12 October
Mallory Knodel
Wout de Natris

Working Groups of the IS3C

1. Security by Design – Internet of Things
2. Education and Skills
3. Procurement and Supply Chain Management and the Business Case
4. Communication – GDC and SDGs
5. “The List”
6. Data Governance and Privacy
7. - - (Consumer Protection)
8. DNSsec and RPKI deployment
9. Emerging Technologies, e.g. A.I., Quantum Computing, Metaverses
10. ...

Procurement and Supply Chain Management and the Business Case

IGF Dynamic Coalition on Internet Standards, Security and Safety



WG3 Mission

Procurement and Supply Chain Management and the Business Case

... for the inclusion of security-related technical standards in public sector procurement contracts and supply chain management of digital technologies.

This multi-stakeholder working group aims to improve the security and safety of the global internet for all by developing **recommendations** and **guidance** for decision makers so that **requirements for security-related technical standards** are included in **public sector procurement contracts** and **supply chain management** of digital technologies.

Meeting global internet security standards is a ubiquitous baseline requirement in any public or private sector procurement and supply chain management policy.

Outcome

Meeting global internet security standards is a ubiquitous baseline requirement in any public or private sector procurement and supply chain management policy.

Objectives

1. Full scope of security standards and procurement challenges and opportunities.

2. Relevant and actionable guidance to require security standards in procurement.

3. Guidance influences public and private sector procurement and supply chain management.

Activities

1.1 Conduct basic desk research to answer “What has been done by others to achieve this project’s outcome”?
1.2 Develop a decision matrix to narrow in on global institutions within the UN IGF’s sphere of influence and impact.
1.3 Collect and document existing procurement and supply chain policies of those institutions, and contacts list.
1.4 Adjust workplan based on findings.

2.1 Circulate a short survey to procurement decision makers on challenges and opportunities in shifting policies.
2.2 Identify areas for improvement in existing procurement and supply chain management policies for internet security standards.
2.3 Develop a guidance document (checklist, issue paper, etc), or suite of materials, fit for purpose.
2.4 Determine areas of future work and adjust workplan.

3.1 Circle back to decision makers with guidance.
3.2 Identify industry spaces, such as cybersecurity trade shows, in which to promote our approach as preventative.
3.3 Promote the IS3C and its future work to decision makers.
3.4 Follow up to document outcomes, if any.

Outputs

Issue paper (2021)

Guidance documents (2022)

Working group growth (ongoing)

A global survey of procurement guidance

The aim of this research is to document what has been done by others and identify actionable areas for developing guidance and future research.

1. First, we conducted basic desk research to answer “What has been done by others on procurement and supply chain management guidance”?
2. Then, we developed a decision matrix to narrow in on global institutions within the UN IGF’s sphere of influence and impact to choose which cases to include in our research.

Final paper is open for review at <https://intgovforum.org>

Terminology

- **Procurement**, in the context of digital technologies, refers to the process of acquiring goods, services, or solutions from external sources to meet the needs and requirements of an organisation.
- **Supply chain management** plays a crucial role in the procurement of digital technologies. It encompasses the coordination and integration of various activities involved in sourcing, procurement, production, and distribution of goods or services.
- **Security standards** are critical in the procurement of digital technologies due to the increasing importance of protecting sensitive information, systems, and networks from cyber threats.

Methods

Desk research answered, “What has been done by others on procurement and supply chain management guidance”?

For each document we reviewed, we asked the following research questions:

- What has been published on procurement and cybersecurity standards already?
- Are there any companies that publish their procurement and supply chain policies?
- What procurement policy/documents focus on internet and digital comms?

Methods (continued)

We sifted the data on existing and previous initiatives to identify

1. common elements of best practice;
2. shared problems barriers; and
3. global north and Global South applicability.

Findings

Those findings were grouped into trends and areas of focus according to the US's National Institute of Standards and Technology's (US NIST) five core cybersecurity functions:

- Identify
- Protect
- Detect
- Respond
- Recover

Conclusions: Best practice awards

- The **GDPR in the European Union** provides common understanding and harmonisation with regards to the security of information systems.
- The Dutch Ministry of the Interior and Kingdom Relations makes mandatory standards deployment. The **‘Pas-Toe-Leg-Uit Lijst’ (comply-or-explain list)** of the Forum Standardisation is a document containing 43 open standards that all governments in the Netherlands have to demand when procuring ICTs.
- **Internet.nl**: The tool used to track standards adoption by an organisation’s website based on three indicators: website, email and connection. The software has been adopted in Australia, Brazil, Denmark and Singapore.

Future work

1. Make use of open cybersecurity standards as points of reference.
2. Compliance of international treaties demonstrates an opportunity for the role of international institutions like the IGF.
3. Many government ministries do not have a standalone document addressing cybersecurity standards in the procurement of ICT and electronic services.
4. Develop frameworks to enhance cybersecurity in the procurement of ICT goods and services for the general public.
5. Proper documentation before and after service provision reduces disruptions.
6. Coordination among industry and public agencies in how these standards are applied.

More information

Authors

- Liz Orembo <lizorembo@gmail.com>
- Mallory Knodel <mallory.knodel@is3coalition.org >

DC IS3C Leadership

- Wout de Natris <wout.denatris@is3coalition.org>
- Mark Carvell <mark.carvell@is3coalition.org>

Read the report here: <https://is3coalition.org/>

WG 5 Prioritizing and listing existing, security-related Internet standards and ICT best practices

Mission statement

IS3C provides decision-takers and procurement officers involved in ICTs procurement with a list containing the most urgent internet standards and related best practices. This assists them to take into account internet security and safety requirements and procure secure by design ICT products, services and devices, making their organisations as a whole more secure and safer.



WG 5 Status report

A team of experts was formed

Members from three continents, four stakeholder groups

A consultation has been announced on 10 October

Until Sunday 5 November, 12.00 UTC

What is consulted?

WG 5 Consultation

Decisions made by IS3C advisory panel:

- Scoping
 - Interoperable, security related, open process and proven
- Categories
 - Data protection and privacy
 - Network and Infrastructure Security
 - Website and (Web) Application Security
 - Communication Security
- Selected standards in concept list

WG 5 next steps

- Consultation document
https://docs.google.com/document/d/1ZC6PBHOREbObHUGopAkPQbIWC_EgLQ8nDyDvULjCwd8/edit?usp=sharing
- Second half November: decision time
- Final report December 2023

Project 2 Create full overview of security standards, outreach starts soon



More information

Wout de Natris <wout.denatris@is3coalition.org>

Trusted Internet India Initiative (T3I)

Satish Babu

About Speaker



- A part of the Internet Governance community since 2009
- Active volunteer with ICANN, ISOC, IEEE and the Computer Society of India
- Presently, a member of ICANN's At-Large Advisory Committee (ALAC)
- Chair, Asia-Pacific School on Internet Governance (APSIG), and co-founder of the India School on Internet Governance (<https://insig.in>), which completed its 8th edition two weeks ago

Background

- The India School on Internet Governance (inSIG, founded: 2016) began cooperating with the Netherlands-based Global Forum for Cyber Expertise (GFCE) from 2018
- inSIG organized GFCE's Internet Infrastructure Initiative (Triple-I) Workshop in 2018, 2019, 2022 and 2023 as Day 0 events of inSIG
- The Triple-I workshop seeks to “...enhance justified trust in the Internet” by building awareness and capacity on Internet-related international standards, norms and best practices
- In its 2023 edition, the Triple-I workshop announced a new initiative that attempts to measure periodically the compliance of Indian websites, DNS and email services to modern security standards (to begin in 2024)

T3I: The context

- India is betting heavily on digital technologies to achieve its growth. It has made several strides in Digital Transformation for Governance, using Digital Public Infrastructure (“India Stack”) and Digital Public Goods
- As one of the most populous country in the world, the India Stack has been so far robust & scalable, and operates at a 1-billion citizen scale on multiple applications including financial, health, and logistics
- Despite this, the level of compliance to many international standards for DNS, web, email are weak, based on a preliminary study conducted by T3I volunteers
- T3I plans to periodically run tests and disseminate results to all stakeholders in the country

Thank You!



Flavio Kenji Yanai & Gilbert Zorello



nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

egi.br

Comitê Gestor da
Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

TOP – *Teste os Padrões in Brazil* (*Test the Standards*)

Flavio Kenji Yanai / Gilberto Zorello

IGF 2023 – Internet Governance Forum - Kyoto, Japan

23/10/12

nic.br

Our Agenda

TOP – Teste os Padrões

- **About NIC.br**
- The Project
- **Program for a Safer Internet**
- **Security Notifications, MANRS and TOP Statistics**
- Implementation remarks



About NIC.br

- ❖ The Brazilian Network Information Center (NIC.br) is a non-profit civil entity that since 2005 has been assigned with the administrative and operational functions related to the .br domain.
- ❖ In addition to providing and maintaining the domain names registration activity quality, **NIC.br** goes beyond similar entities in other countries, investing in actions and projects that bring a series of benefits to the improvement of activities related to the available Internet infrastructure in Brazil, with a revenue collected exclusively through the provision of services.
- ❖ Some of our efforts are focused on all sectors of Brazilian society, disseminating knowledge about best practices to be adopted in networks and related areas. In some cases, we strengthen relationships with private, governmental, and nonprofit entities to encourage the adoption of best practices.

TOP – Teste os Padrões

The Project

Developed by NIC.br to disseminate the best security practices in Brazil for web sites, e-mail services and user connection to Internet

Uses the open-source code provided by the Dutch implementation of Internet.nl with a web interface in Portuguese to attend Brazilian users in local language

The project is part of the **Program for a Safer Internet** in Brazil, which works with ISPs and incumbent operators to disseminate the best security practices that they should implement on their respective networks.

Start of operation in Dec/21

Access: <https://top.nic.br>



<https://top.nic.br>

Program for a Safer Internet Objectives

Act in support of the Internet technical community

- Reduction of Denial of Service attacks
- **Improving Network Routing Security**
- Spread DNS security best practices
- **Disseminate best security practices for configuring websites and email services**
- Encourage the implementation of IPv6 in final users and services on the network



Program for a Safer Internet Plan of Actions

Performed by NIC.br

- Several internal departments of NIC.br participate in the Program (CERT.br, CEPTRO.br, Registro.br, IX.br, Systems)
- **Creation of teaching materials and good practices**
- Raising awareness in the technical community through lectures, courses and training
- **Direct interaction with network operators through bilateral meetings to explain how to implement the best practices recommended in each situation**
- Definition of KPIs to monitor the effectiveness of actions



Program for a Safer Internet

Bilateral meetings with ISPs and incumbents

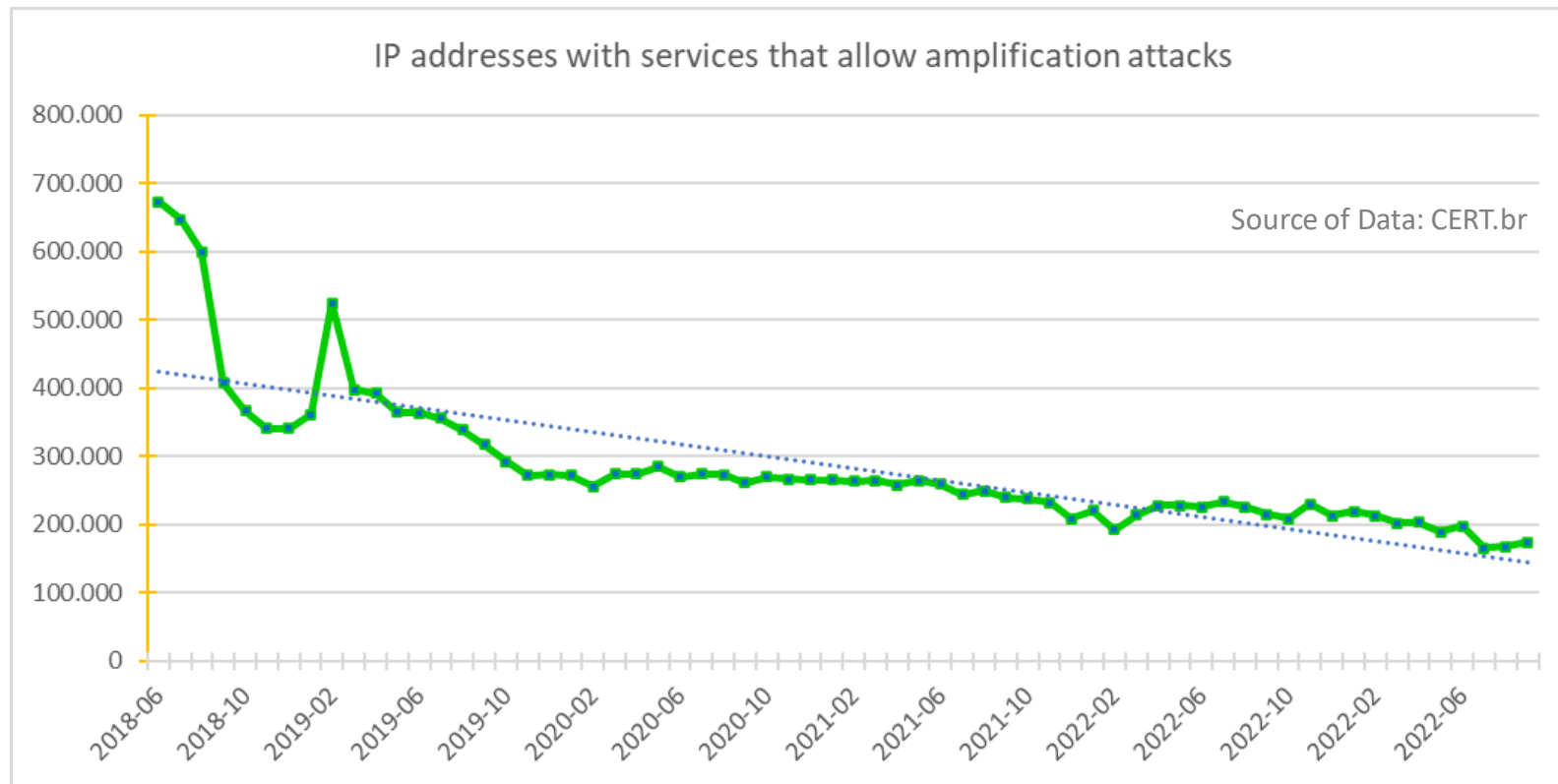


- Bilateral online meetings with those **responsible for the ASes** with the highest number of IP addresses notified
- **Program actions discussed in bilateral meetings:**
 - Correction of misconfigured services reported by CERT.br, which can be abused to take part in DDoS attacks
 - **Adoption of Good Routing Practices (MANRS)**
 - Verification of adoption of best configuration practices **recommended by TOP** (final user, Web Site and E-mail services)
 - **Presentation of measurements, by AS, on the status of adoption of recommended good practices**

Program for a Safer Internet

Statistics of Notifications of IP Addresses

- Quantity of IP addresses notified with misconfigured services



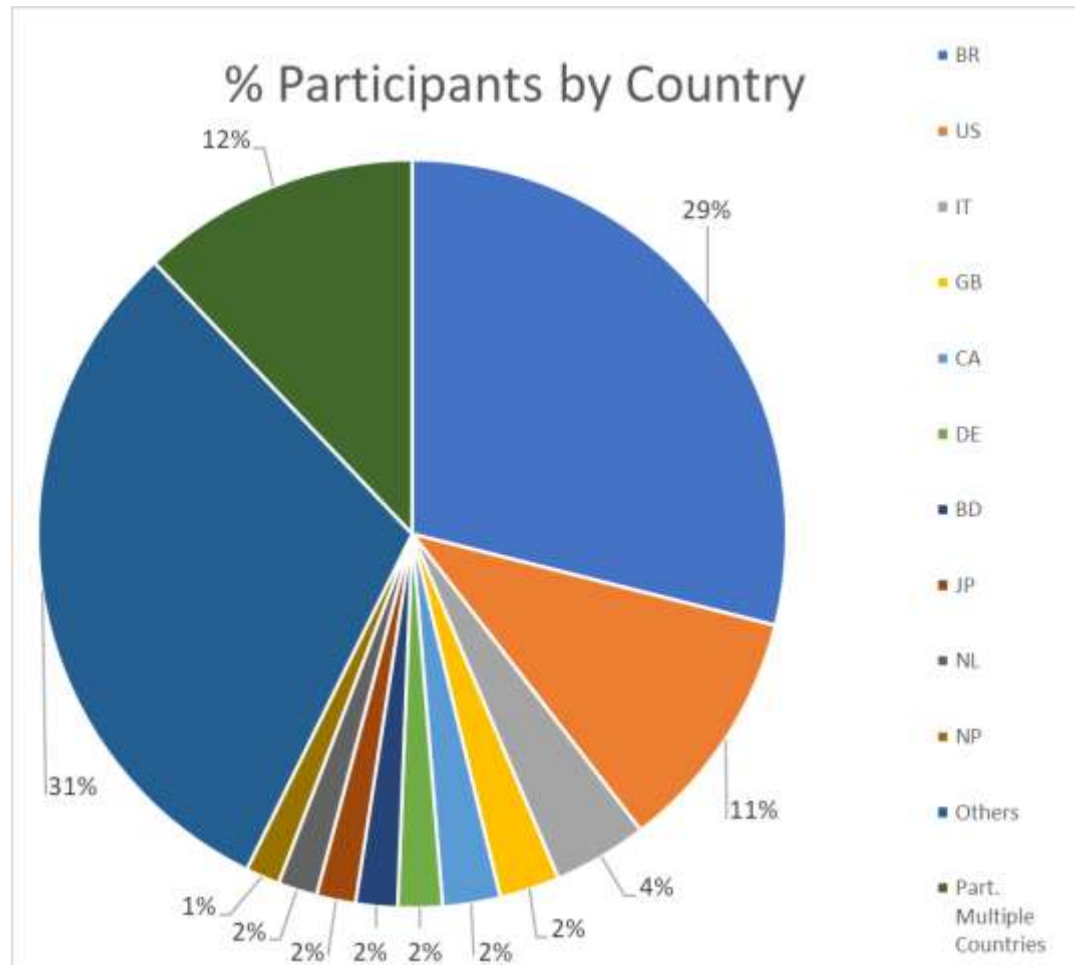
Reduction of in misconfigured IP addresses since the start of the Program

Program for a Safer Internet

Statistics of MANRS Participants by Country



- Distribution by country of providers participating in the MANRS initiative



Total of MANRS participants: 885

Participants in Brazil: 256 (Set/23)

206 (2022)

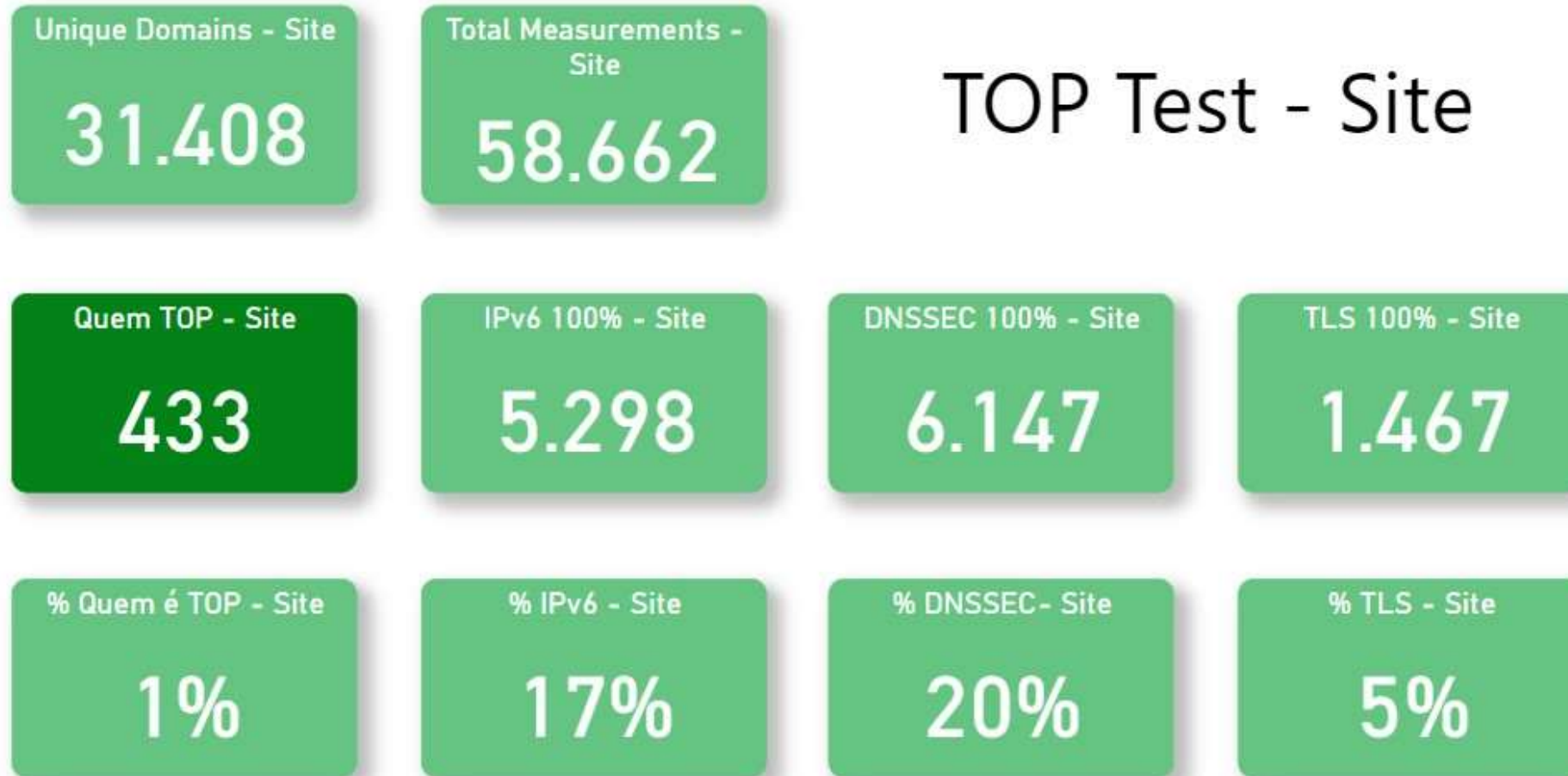
174 (2021)

140 (2020)

Source: <https://www.manrs.org/netops/participants/> Access set/23

Program for a Safer Internet

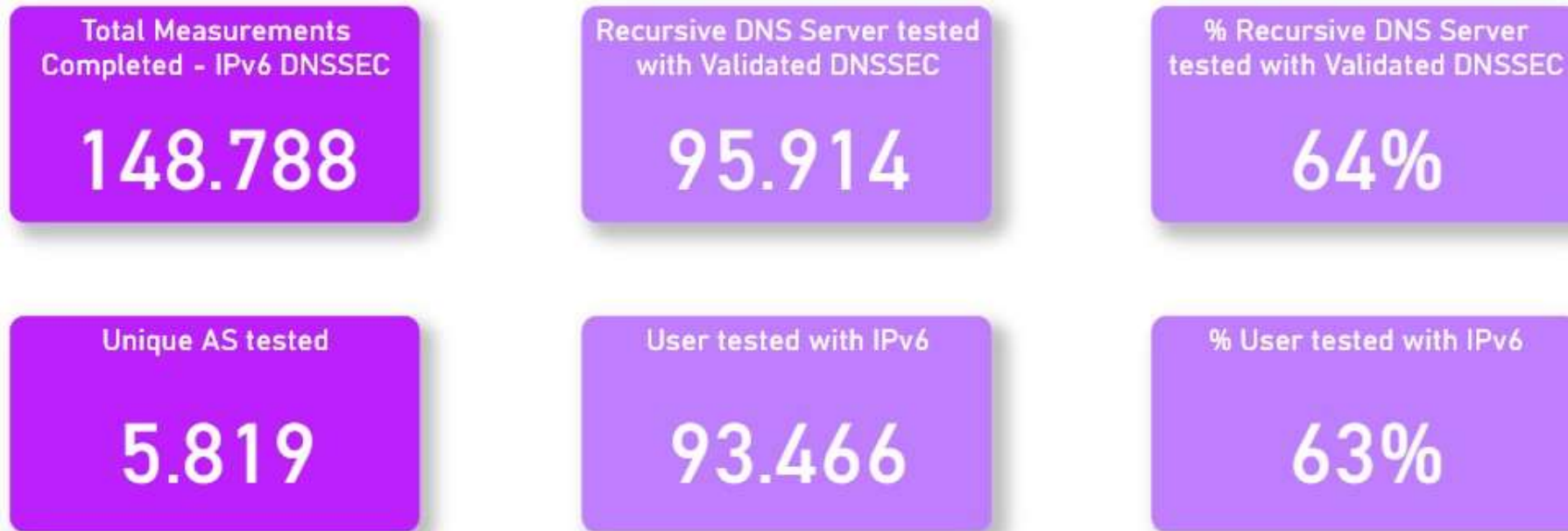
Statistics of TOP for Web Site Tests



Program for a Safer Internet

Statistics of TOP for Connections Tests

TOP Test - IPv6 DNSSEC - Recursive and User Network



Total IPv6 measurements 100%

Program for a Safer Internet

Statistics of TOP for Email Tests

TOP Test - E-mail

Unique Domains -
Email

16 Mil

29.025

Medições - E-mail

Quem é TOP - E-mail

71

IPv6 100% - E-mail

1.851

DNSSEC 100% -
E-mail

1.837

Authenticity Marks
100% - E-mail

2.259

STARTTLS 100% -
E-mail

89

% Quem é TOP -
E-mail

0%

% IPv6 - E-mail

12%

% DNSSEC - E-mail

12%

% Authenticity Marks
- Email

14%

% STARTTLS - E-mail

1%

TOP – Associations of Brazilian ISPs and Academia



A CONECTIVIDADE AO SEU ALCANCE



TOP – Teste os Padrões

Implementation remarks

- The software was delivered in Dec/21, currently is running 1.4 version of Internet.nl
- **The 1.7 version of Internet.nl is implemented and in phase of validation**
- The best practices recommended by the tool are recommendations from NIC.br to the technical community in Brazil
- **The tool is being disseminated together with the Program for a Safer Internet at technical events and for specific sectors such as government, academia and Internet operators**



TOP – Teste os Padrões

Implementation remarks

- The accounting area of Brazil's legislature carried out tests of the websites and email services used by the government
- **The TOP tool provides important indication of the implementation status of recommended best practices and provides a baseline for operators to implement them in their networks**
- Brazil has continental dimensions and it is a challenge to keep up with the evolution of the use of standards





ISC Procurement Consultation Document

More information on
IS3C: <https://is3coalition.org/>

Thank you

<https://top.nic.br>

@ gzorello@nic.br

@ yanai@nic.br

2023 October, 12

nic.br **cgi.br**

www.nic.br | www.cgi.br