Procuring Modern Security Standards by Governments and Industry
Speakers and panel members

Olaf Kolkman: Internet Society, moderator

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

Annemieke Toersen: advisor of Netherlands Standardization Forum

Satish Babu, ICFOSS, SIFFS, ISOC, ICANN CSI

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

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

Flavio Kenji Yanai, NIC Brasil, software engineer

Gerben Klein Baltink, voorzitter Platform Internet Standaarden
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

13:30 – 13:40
Introduction by Olaf Kolkman

13:40 – 13:55
the Role of Open Standards particularly in procurement, experiences in the Netherlands, by Gerben Klein Baltink & Annemieke Toersen

13:55 – 14:15
Procurement and Supply Chain Management and the Business Case, by Wout de Natris

14:15 – 14:25
Questions in the audience
Programme – part 2

14:25 – 14:35
Satish Babu, perspectives from India

14:35 – 14:45
Gilberto Zorello & Flavio Kenji Yana, perspectives from Brasil

14:45 – 14:59
Panel discussion

15:00
Closing remarks
• Platform Internet Standards in the Netherlands
• Adoption
• Tooling
Procuring modern security standards by governments & industry

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

1. Mandatory
   - Comply-or-explain regarding new investments
   - Public commitments with implementation deadline
   - Mandatory by law

2. Co-operation
   - Public/private
   - Contact with vendors
   - Knowledge exchange

3. Monitor
   - Review procurement docs
   - Measurements
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,  
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), sikkerpånettet.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)
3. Monitoring using Internet.nl
If you don’t ask it...
You don’t get it.
Questions?

- More info:
  - https://www.forumstandaardisatie.nl
  - https://internet.nl/
INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

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

<table>
<thead>
<tr>
<th></th>
<th>1. Full scope of security standards and procurement challenges and opportunities.</th>
<th>2. Relevant and actionable guidance to require security standards in procurement.</th>
<th>3. Guidance influences public and private sector procurement and supply chain management.</th>
</tr>
</thead>
</table>

### Activities

<table>
<thead>
<tr>
<th></th>
<th>1.1 Conduct basic desk research to answer “What has been done by others to achieve this project’s outcome”?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.2 Develop a decision matrix to narrow in on global institutions within the UN IGF’s sphere of influence and impact.</td>
</tr>
<tr>
<td></td>
<td>1.3 Collect and document existing procurement and supply chain policies of those institutions, and contacts list.</td>
</tr>
<tr>
<td></td>
<td>1.4 Adjust workplan based on findings.</td>
</tr>
<tr>
<td></td>
<td>2.1 Circulate a short survey to procurement decision makers on challenges and opportunities in shifting policies.</td>
</tr>
<tr>
<td></td>
<td>2.2 Identify areas for improvement in existing procurement and supply chain management policies for internet security standards.</td>
</tr>
<tr>
<td></td>
<td>2.3 Develop a guidance document (checklist, issue paper, etc), or suite of materials, fit for purpose.</td>
</tr>
<tr>
<td></td>
<td>2.4 Determine areas of future work and adjust workplan.</td>
</tr>
<tr>
<td></td>
<td>3.1 Circle back to decision makers with guidance.</td>
</tr>
<tr>
<td></td>
<td>3.2 Identify industry spaces, such as cybersecurity trade shows, in which to promote our approach as preventative.</td>
</tr>
<tr>
<td></td>
<td>3.3 Promote the IS3C and its future work to decision makers.</td>
</tr>
<tr>
<td></td>
<td>3.4 Follow up to document outcomes, if any.</td>
</tr>
</tbody>
</table>

### Outputs

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.
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?
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/1ZC6PBHOREbObHUGopAkPQblWC_EgLQ8nDvULjCwd8/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).
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 countries 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
TOP – Teste os Padrões in Brazil (Test the Standards)

Flavio Kenji Yanai / Gilberto Zorello

IGF 2023 – Internet Governance Forum - Kyoto, Japan

23/10/12
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
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 misconfigured IP addresses since the start of the Program

Source of Data: CERT.br
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/ Acess set/23
# Program for a Safer Internet

## Statistics of TOP for Web Site Tests

<table>
<thead>
<tr>
<th>Metric</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Domains</td>
<td>31,408</td>
</tr>
<tr>
<td>Total Measurements</td>
<td>58,662</td>
</tr>
<tr>
<td>Quem TOP</td>
<td>433</td>
</tr>
<tr>
<td>IPv6 100%</td>
<td>5,298</td>
</tr>
<tr>
<td>DNSSEC 100%</td>
<td>6,147</td>
</tr>
<tr>
<td>TLS 100%</td>
<td>1,467</td>
</tr>
<tr>
<td>% Quem é TOP</td>
<td>1%</td>
</tr>
<tr>
<td>% IPv6</td>
<td>17%</td>
</tr>
<tr>
<td>% DNSSEC</td>
<td>20%</td>
</tr>
<tr>
<td>% TLS</td>
<td>5%</td>
</tr>
</tbody>
</table>

**TOP Test - Site**
### Program for a Safer Internet
### Statistics of TOP for Connections Tests

**TOP Test - IPv6 DNSSEC - Recursive and User Network**

<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
<th>Recursive DNS Server</th>
<th>% Recursive DNS Server</th>
<th>Unique AS tested</th>
<th>User tested with IPv6</th>
<th>% User tested with IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Measurements Completed - IPv6 DNSSEC</td>
<td>148,788</td>
<td>95.914</td>
<td>64%</td>
<td>5,819</td>
<td>93.466</td>
<td>63%</td>
</tr>
<tr>
<td>Recursive DNS Server tested with Validated DNSSEC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Program for a Safer Internet

#### Statistics of TOP for Email Tests

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Domains - Email</td>
<td>16 Mil</td>
</tr>
<tr>
<td>IPv6 100% - E-mail</td>
<td>1.851</td>
</tr>
<tr>
<td>DNSSEC 100% - E-mail</td>
<td>1.837</td>
</tr>
<tr>
<td>Authenticity Marks 100% - E-mail</td>
<td>2.259</td>
</tr>
<tr>
<td>% Quem é TOP - E-mail</td>
<td>0%</td>
</tr>
<tr>
<td>% IPv6 - E-mail</td>
<td>12%</td>
</tr>
<tr>
<td>% DNSSEC - E-mail</td>
<td>12%</td>
</tr>
<tr>
<td>% Authenticity Marks - Email</td>
<td>14%</td>
</tr>
<tr>
<td>% STARTTLS - E-mail</td>
<td>1%</td>
</tr>
</tbody>
</table>
TOP – Associations of Brazilian ISPs and Academia
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

www.nic.br | www.cgi.br