Forum Standaardisatie

Standaard Samenwerken

Increasing IPv6 adoption within the Dutch government

Robin Gelhard

Advisor on ICT Standardisation

Forum Standaardisatie

Standaard Samenwerken

Netherlands Standardisation Forum

- Thinktank on interoperability that advises Dutch government
- Members from government, businesses and science
- Goal: interoperability and vendor neutrality
- Open standards are the norm
- Maintains list with open standards
  - 42 mandatory for government (comply-or-explain)

Forum Standaardisatie

Standaard Samenwerken

Promoting modern Internet standards

IPv6, DNSSEC, HTTPS, DMARC, DKIM and SPF, STARTTLS and DANE, RPKI

No single organisation can drive adoption: public/private cooperation

Forum Standaardisatie

Standaard Samenwerken

Why IPv6?

- Growth and innovation of the Internet
- More direct and faster digital government services
- Fraud detection and prevention

However:

- The individual and social utility of IPv6 increases as IPv6 is more supported.
- There is a 'first mover disadvantage’.
- This leads to a market failure, which means that adoption is slow or slow.
- Among other things, the government can promote adoption by setting a good example.

Forum Standaardisatie

Standaard Samenwerken

IPv6 and Dutch government timeline

- November 2010: IPv6 op de ‘pas toe of leg uit’-lijst
- Oktober 2019: Declaration of intent to speed up implementation of IPv6, signed by government digital infrastructure providers, shared service providers, and several suppliers
- April 2020: On the advice of the Standardisation Forum, the Digital Government Policy Board ratifies the following target agreement:

“All government websites and government email domains must be fully reachable over IPv6 by the end of 2021, in addition to IPv4.”

Forum Standaardisatie

Standaard Samenwerken

Policy measures for government entities

Required by law

(under the Digital Government Act, not yet ratified)

Target agreements

(obligation to use before a deadline)

‘Comply or explain’ policy

(purchase obligation >50.000 euro)

Forum Standaardisatie
Standaard Samenwerken

Target agreements for Internet standards

Deadline	Standards
End of 2017	HTTPS and TLS: secure connections of websites 'with sensitive data' DNSSEC: domain name data integrity SPF: authenticity mechanism to prevent mail spoofing DKIM: authenticity stamp to prevent mail spoofing DMARC: mail spoofing prevention policy and reporting mechanism
End of 2018	HTTPS, TLS and HSTS in accordance with the TLS guidelines of the Dutch NCSC: secure connections of all websites
End of 2019	STARTTLS en DANE: encryption of email traffic SPF and DMARC: setting strict policies for these email standards
End of 2021	IPv6 (naast IPv4): modern internet addressing of government websites and government e-mail domains

Forum Standaardisatie

Standaard Samenwerken

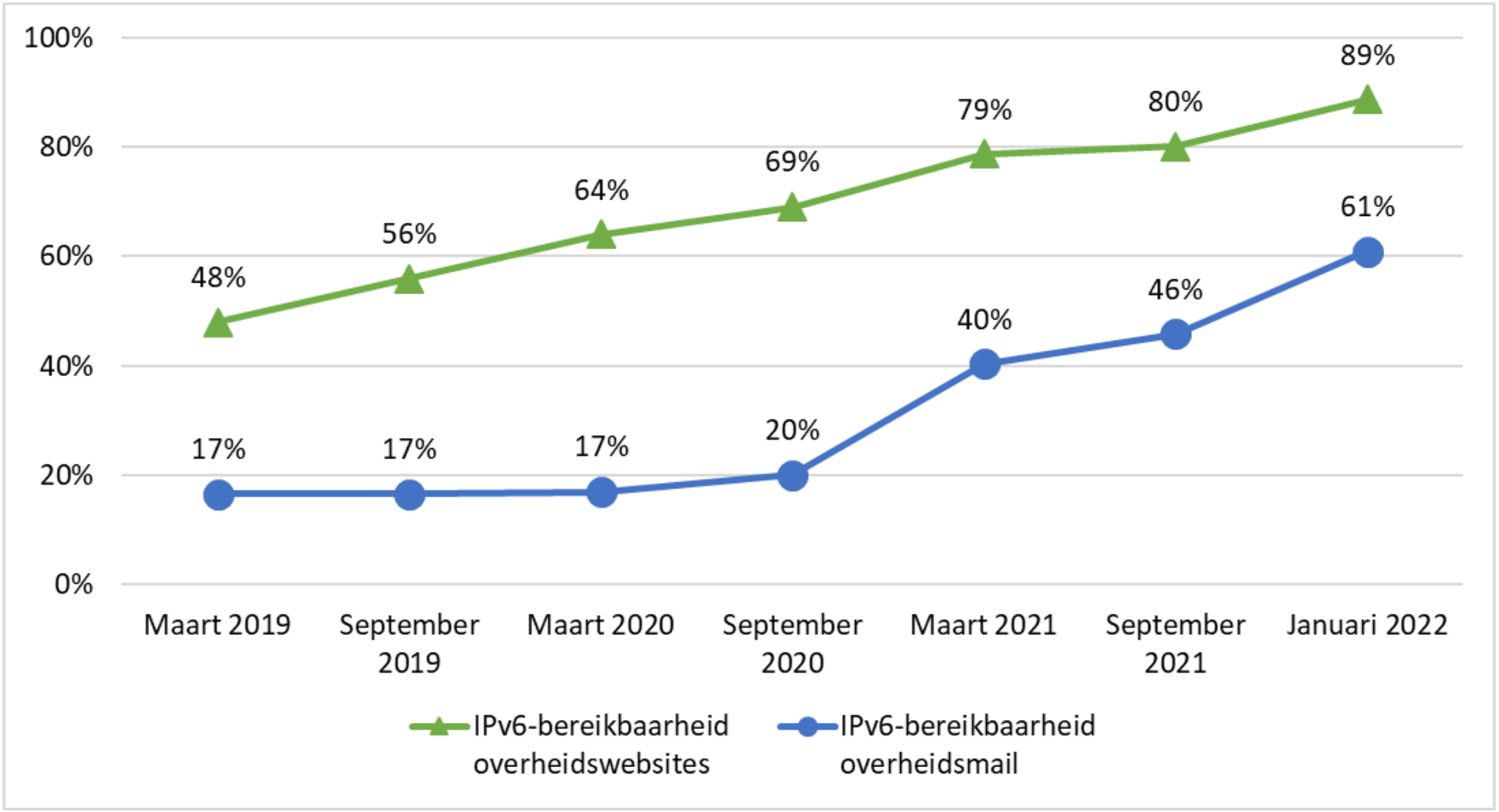
What do we measure?

IPv6 reachability of websites	We test whether all name servers (at least two) and at least one web server have an IPv6 address and are reachable. It is also tested whether the IPv6 website resembles the IPv4 website.
IPv6 reachability of email systems	We test whether all name servers (at least two) of the e-mail domain and all mail servers (MX) have an IPv6 address and are reachable.

Forum Standaardisatie
Standaard Samenwerken

Sample size:
559 domain names:
- *Central government*
- *Local governments*

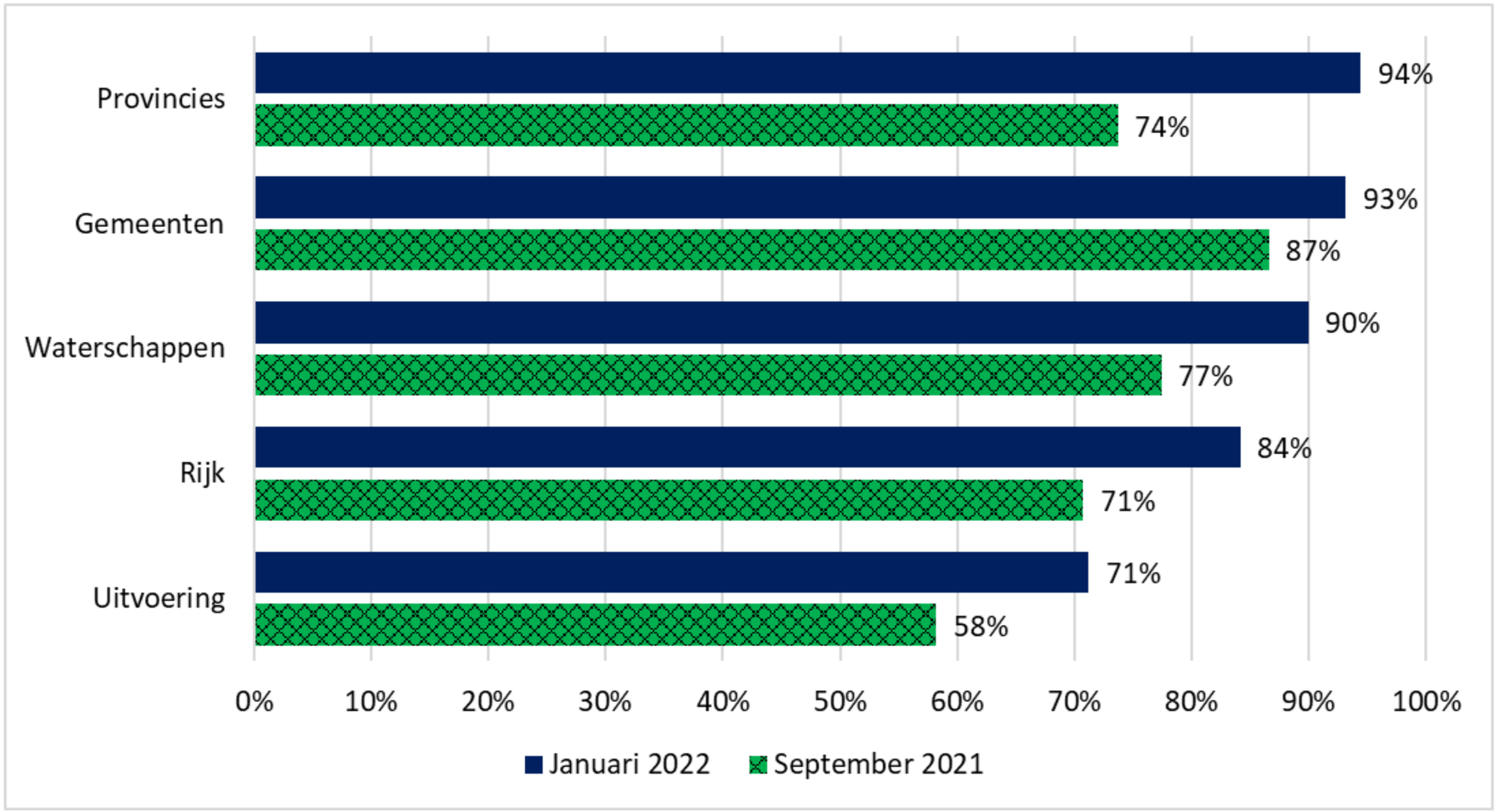
Trend and ‘result’



Forum Standaardisatie

Standaard Samenwerken

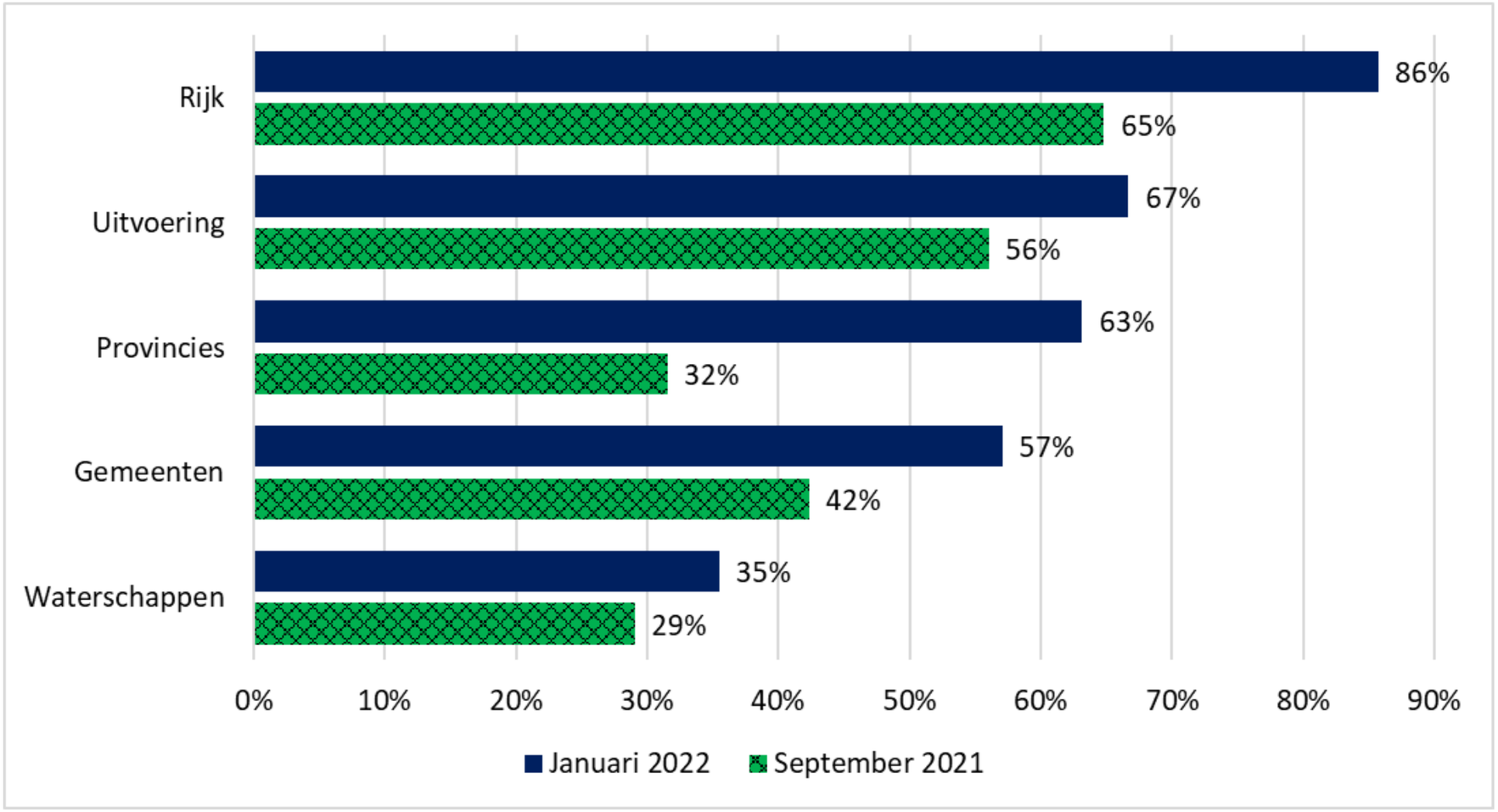
IPv6-reachability **websites**



Forum Standaardisatie

Standaard Samenwerken

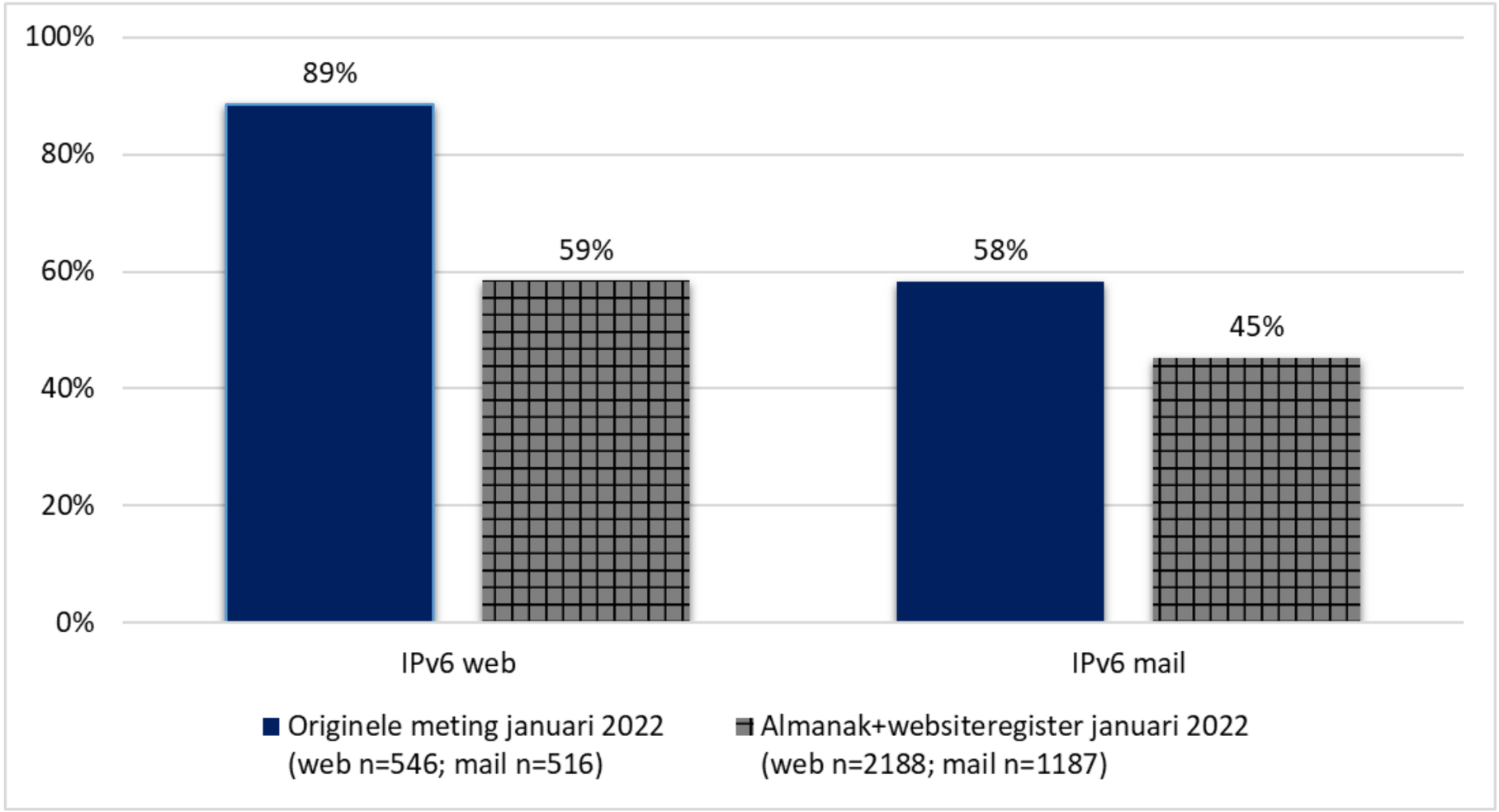
IPv6-reachability **e-mail**



Forum Standaardisatie

Standaard Samenwerken

Broader measurement among government domains



Forum Standaardisatie

Standaard Samenwerken

Recommendations to our government

- directly address lagging government organizations
- directly address lagging shared service providers
- point out to governments that use Microsoft Office 365 (Exchange Online) the option of activating IPv6
- to realize an IPv6 obligation for websites and e-mail through an executive order, on the basis of the pending Digital Government Act

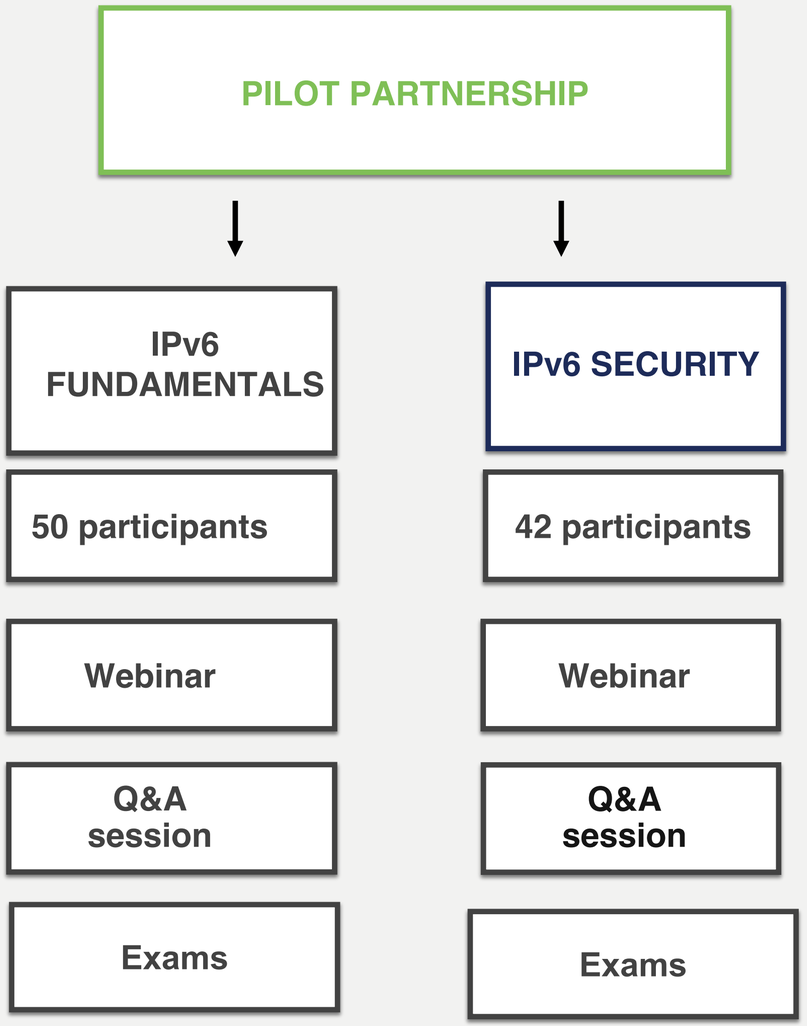
Forum Standaardisatie

Standaard Samenwerken

Partnership with the RIPE NCC

- Initiated in October 2021
- Aims to support the IPv6 transition from a skills perspective
- Based on the existing RIPE NCC Certified Professionals exams supported by the RIPE NCC Academy e-learning platform and live webinars with trainers
- Pilot for two programmes:
  - IPv6 Fundamentals which ran from Nov – March
  - IPv6 Security which ran from Jan - May
- Regular feedback with Forum Standaardisatie and the VNG IPv6 team

Pilot Structure and Feedback



SETUP:

Pilot with two tracks for various organisations in the Dutch government led by Logius from Nov 2021 – May 2022

- Central government
- Local government
- Specific related organisations

FINDINGS:

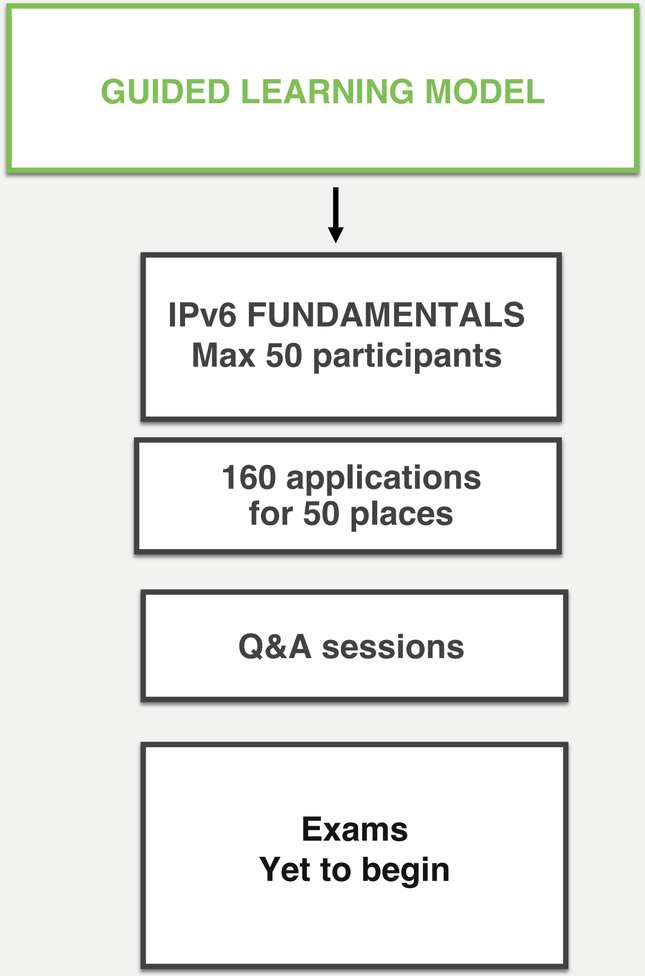
Interest from participants in the tracks, the IPv6 Fundamentals trac was oversubscribed, IPv6 Security included participants from the Dutch National Cyber Security Centre.

Participants could attend a webinar and Q&A sessions with RIPE NCC trainers

They could also opt to get certified by taking an exam

Based on the positive outcomes, the cooperation continued in an extended roll-out

Ongoing Partnership



SETUP:

IPv6 Fundamentals pilot with the RIPE NCC Academy course as the main training element, supported by weekly one hour check-in sessions with RIPE NCC trainers:

- Short overview of the units studied that week
- Q&A on the learned materials

CONCLUSIONS SO FAR:

- High interest in the course, oversubscribed with limited promotion
- Weekly Q&A sessions well attended and reviewed
- Good interaction and questions during the sessions

Forum Standaardisatie and RIPE NCC are planning additional activities together in the Fall.

Forum Standaardisatie

Standaard Samenwerken

Thank you for your attention! :-)

Q&A