RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Internet Standards - The IETF

Mirjam Kühne, RIPE NCC, Senior Community Builder

IETF

Internet Engineering Task Force

The IETF mission

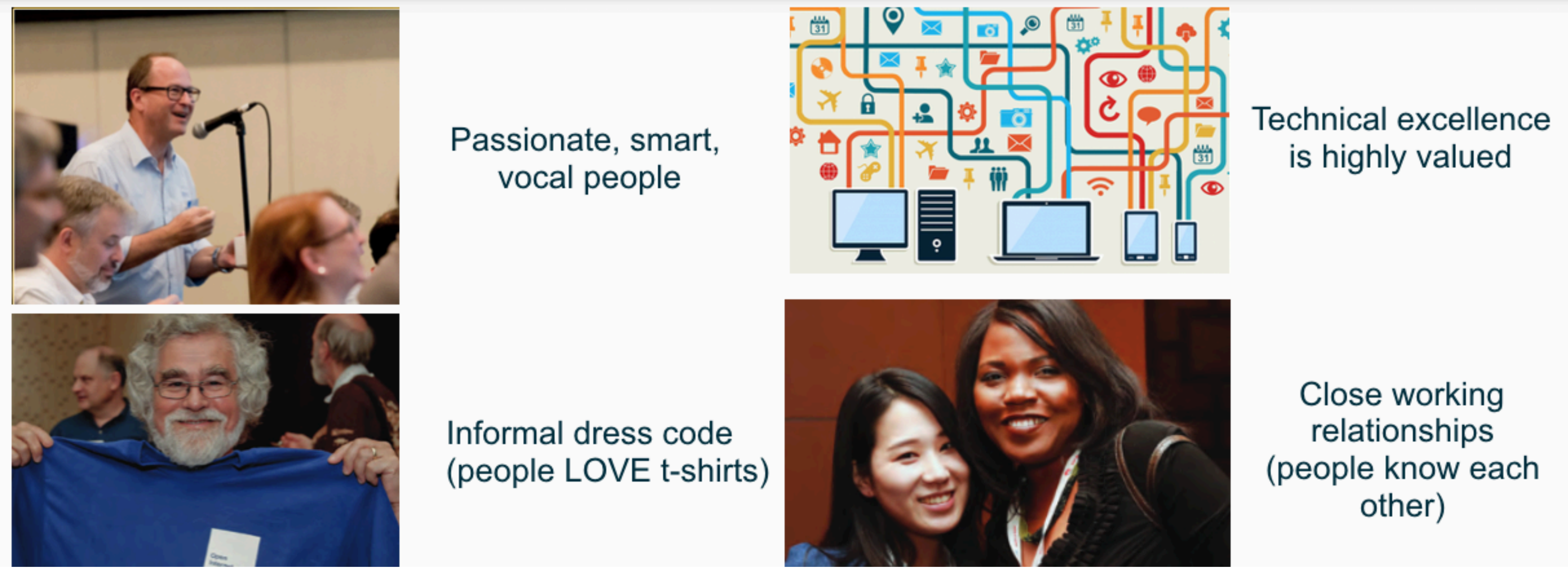
- The Mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. (RFC 3935)

- Loosely self-organised group of people who contribute to the engineering and evolution of Internet technologies (The Tao)

The IETF is a little different ..

- **A Standards Development Organisation (SDO)**
  - Focus on Internet technologies: email, ftp, http, dns
  - Other SDOs: ITU, IEEE, ETSI, W3C
- **No formal membership**
  - People participate as individuals
- **No formal voting (instead: humming)**
- **No formal government role**
  - Driven by market adoption

IETF culture



Passionate, smart, vocal people

Technical excellence is highly valued

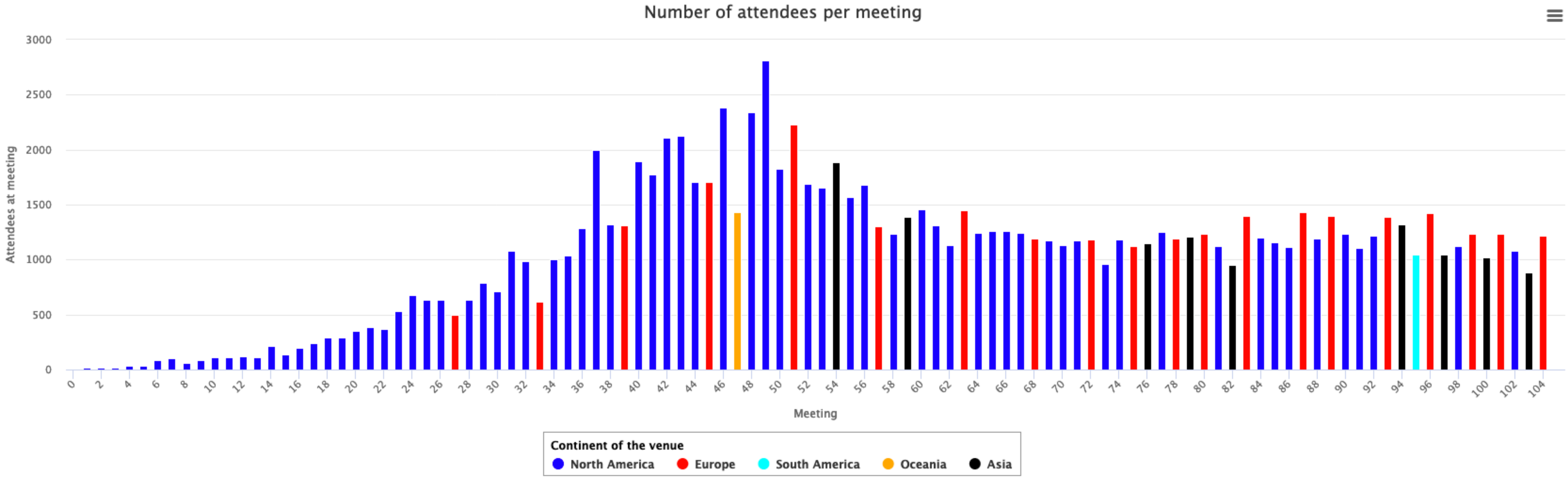
Informal dress code (people LOVE t-shirts)

Close working relationships (people know each other)

Who participates in the IETF?

- Anybody can participate
- Typically network designers, operators, vendors, and researchers
- Working on evolution of the Internet architecture and the smooth operation of the Internet
- Pretty international

IETF participation



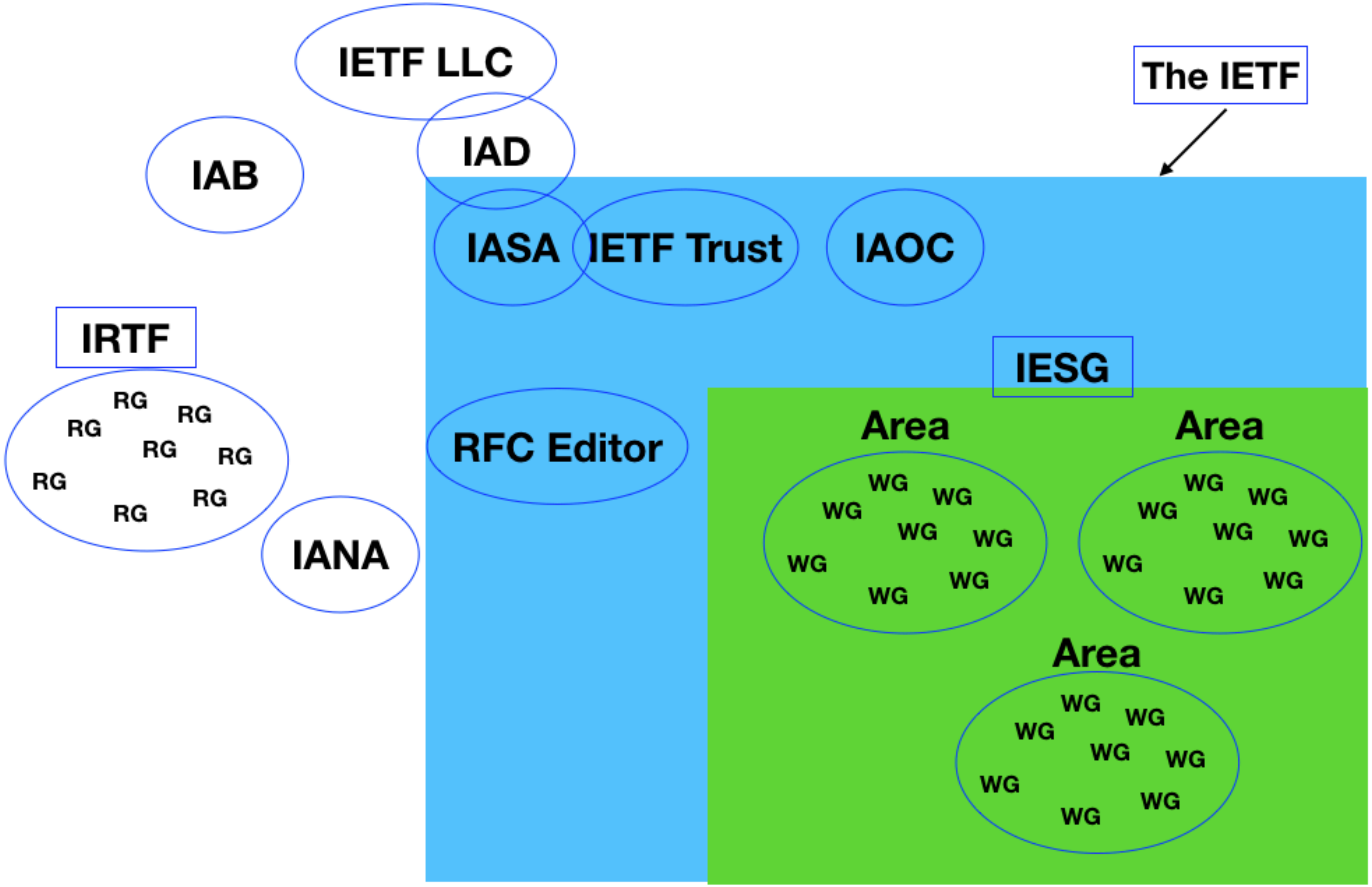
How does it work?

- **Technical work done in Working Groups (~ 130)**
- **Organised by topical areas (currently 7)**
- **Three face-to-face meetings per year**
  - 1,000 - 1,400 participants
  - Good remote participation facilities
- **Most work done on mailing lists**
  - Open to anybody!

IETF areas

Applications and Real-Time (ART)	- Application protocols and architectures - Real-time (communication) and non-real-time
Transport (TSV)	- Mechanisms related to data transport on the Internet - Includes congestion control
Routing (RTG)	- Routing and signalling protocols
Internet (INT)	- IPv4/IPv6, DNS, DHCP, mobility
Operations and Management (OPS)	- Network management - Operations: IPv6, DNS, security, routing
Security (SEC)	- Security protocols and mechanisms
General (GEN)	- Activities focused on supporting and updating IETF processes

IETF structure



Alphabet soup

- **IESG: Internet Engineering and Steering Group**
  - Responsible for technical management of IETF activities
- **IRTF: Internet Research Task Force**
  - Focused on longer-term research topics
- **IAB: Internet Architecture Board**
  - Oversight of Internet architecture and standards process
- **IETF LLC: IETF Limited Liability Company**
  - Legal home for the above; admin and fiscal support

IETF and consensus

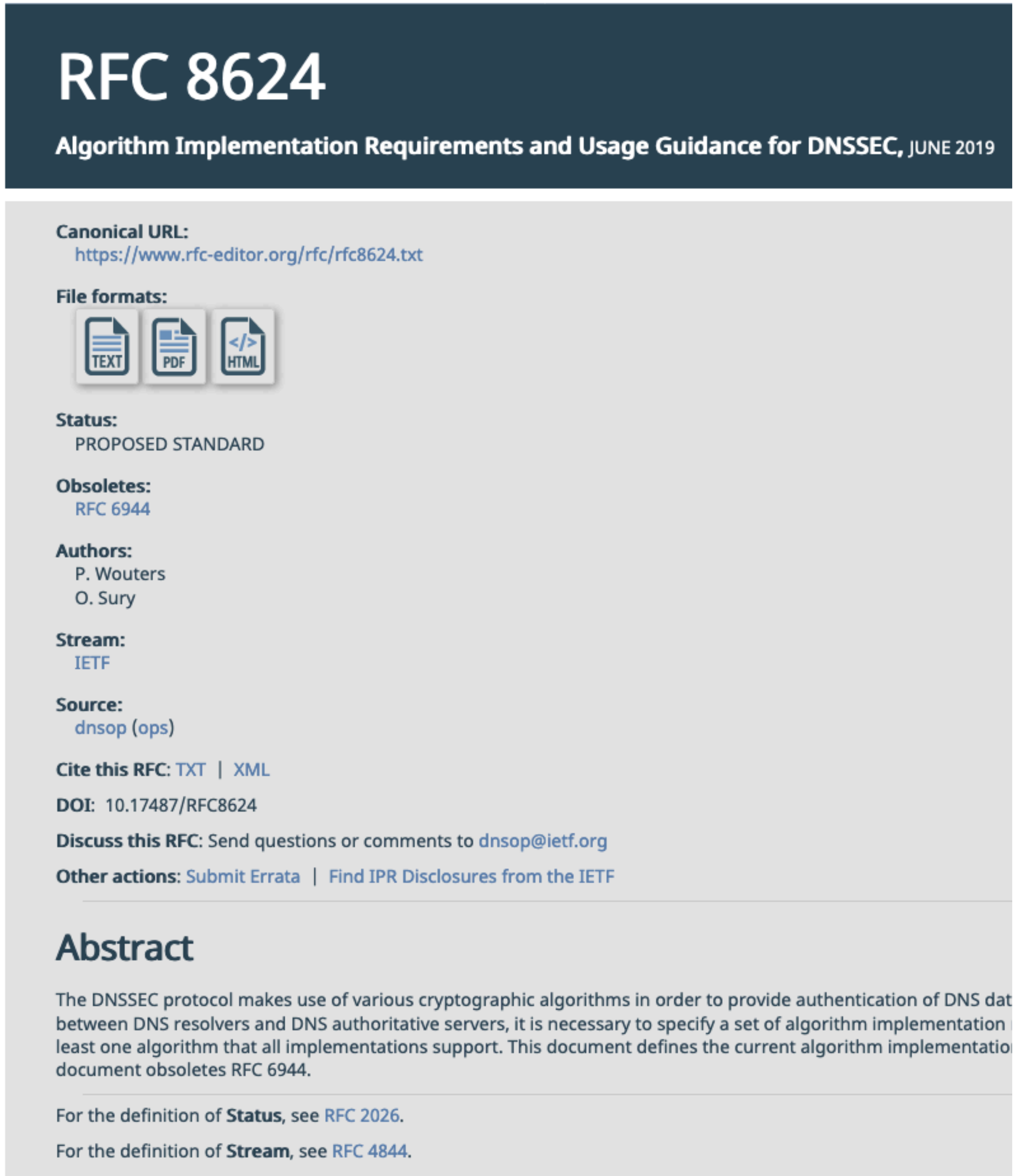
- **IETF mantra:**
  - “We reject kings, presidents and voting. We believe in rough consensus and running code.”
- **Consensus is achieved when all issues are addressed**
  - But they are not all necessarily accommodated
- **Dissenting options are heard, but are not controlling**
- **Humming: a way to measure consensus (anonymously)**
- **“On Consensus and Humming in the IETF” (RFC 7282)**

Requests for Comments - RFCs

- **All IETF documents are open and freely accessible**
- **Not all RFCs Are Standards (RFC 1796)**
- **Categories**
  - Proposed Standards and Full Standards
  - Best Current Practices (BCPs)
  - Informational
  - Experimental
  - Historic

RFCs

- RFC Index:
  - https://www.rfc-editor.org/rfc-index.html
  - https://www.rfc-editor.org/info/rfc8624



RFC 8624

Algorithm Implementation Requirements and Usage Guidance for DNSSEC, JUNE 2019

Canonical URL:
https://www.rfc-editor.org/rfc/rfc8624.txt

File formats:

Status:
PROPOSED STANDARD

Obsoletes:
RFC 6944

Authors:
P. Wouters
O. Sury

Stream:
IETF

Source:
dnsop (ops)

Cite this RFC: TXT | XML

DOI: 10.17487/RFC8624

Discuss this RFC: Send questions or comments to dnsop@ietf.org

Other actions: Submit Errata | Find IPR Disclosures from the IETF

Abstract

The DNSSEC protocol makes use of various cryptographic algorithms in order to provide authentication of DNS dat
between DNS resolvers and DNS authoritative servers, it is necessary to specify a set of algorithm implementation
least one algorithm that all implementations support. This document defines the current algorithm implementatio
document obsoletes RFC 6944.

For the definition of **Status**, see RFC 2026.

For the definition of **Stream**, see RFC 4844.

Other IETF events

- Hackathons
- Code Sprints
- BoFs
- Tutorials
- Plenaries

The Tao of the IETF

- **Describes many aspects of the IETF**
  - Especially useful for newcomers
  - Makes participation more productive and fun
- **Talks about Working Groups, Mailing Lists, Meetings, Running Code, Online Tools, BoFs and RFCs and more**
  - https://www.ietf.org/about/participate/tao/ (recently updated)
- **Translations, including Arabic (2012 version)**
  - http://www6.ietf.org/tao-translated-ar.html

Remote participation

- You can participate remotely
  - Registration, presentation
  - Chat rooms
  - Video streaming
- https://www.ietf.org/about/participate/
  - How to get started
  - Tutorials on technical and procedural topics

Main take-aways

- **Bottom-up, voluntary**
  - Participation as individuals
- **Competitors work together to find best solution for all**
  - Consensus via humming (anonymous)
- **Market decides about what becomes a standard**
  - Sometimes multiple solution for same problem
- **Not a legal entity**
  - Volunteer platform

Current discussions

DNS and privacy

Some history: RFC 2804

- In 1999 the IETF was working on media gateway protocols
- US Law Enforcement asked the IETF to make protocols compliant with the US Communications Assistance for Law Enforcement Act (CALEA)
- In the end the IETF decided not to follow this request
- “IETF Policy on Wiretapping” (RFC 2804, May 2000)

Some more history: RFC 7258

- **After Edward Snowden's revelations, the IETF took a strong position:**
  - "Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible."
- **Pervasive Monitoring Is an Attack (RFC 7258, May 2014)**
  - http://www.circleid.com/posts/20190407_dns_privacy_at_ietf_104/ by Geoff Huston

DNS surveillance

- **Many actors seem to be looking at the DNS**
  - To observe what we all do online and to suggest what services we can access
- **Can we stop DNS surveillance completely?**
  - Probably not
- **But we can make it harder to collect individual profiles of activity**

Why do actors use the DNS for that?

- **DNS name resolution protocol is unencrypted**
  - Anyone can see transactions on the wire
  - Anyone can intercept DNS queries
  - And every Internet transaction starts with a DNS query
- **IETF DNS Private Exchange WG (dprive)**
  - Develops mechanisms to provide confidentiality to DNS transactions
  - Addresses concerns surrounding pervasive monitoring (RFC 7258)

Solutions to enhance DNS privacy (1)

- **QNAME Minimisation (RFC 7816)**
  - DNS resolver no longer sends the entire original query name to the upstream name server
  - Instead it sends only parts of the hierarchy

Hi Root server, I want to know the nameservers for com

Sure, here are the servers for .com

Hi .com server, I want to know the nameservers for example.com

Sure, here are the servers for example.com

Hi example.com server, I want to resolve www.example.com

Sure – its 93.184.216.34

Solutions to enhance DNS privacy (2)

- **DNS over TLS - DoT (RFC 7858, RFC 8310)**
  - TLS is a TCP ‘overlay’ that adds server authentication and session encryption to TCP
  - Client validates identity of server
  - The privacy is relative, as the recursive resolver still knows all your DNS queries
  - Uses port 853 - can easily be blocked by middleware
  - Some DNS recursive resolvers support DNS over TLS (e.g. BIND, Unbound)

DoT - disadvantages

- **Specialised services available to a few technical people**
  - But that might be changing as more providers offer it by default
- **Can easily be blocked (port 853)**
- **Prevents surveillance on the wire, but still shares your DNS activity with the DoT service provider**
  - Still better than not having any encryption

Solutions to enhance DNS privacy (3)

- **DNS over HTTPS - DoH (RFC 8484)**
  - Very similar to DoT, but:
  - Uses port 443 (HTTPS) - makes it difficult to distinguish from HTTPS traffic
  - Not turned on by user or ISP, but by browser or application vendor
  - Therefore bypasses the operating system and its settings
- **Could become “mainstream" service used by potentially billions of end users**

DoH - disadvantages

- **The device-to-resolver connection is encrypted and hidden inside Web traffic**
- **Each application can operate a different DNS resolver**
  - DNS becomes application level services (instead of networking service)
  - Makes it hard to debug for your ISP
- **Each application gains more control over your resolver choice**
  - Application/browser vendors can effectively dominate the Internet's namespace

Main issues around Dot and DoH

- Unencrypted vs. encrypted
- Business model: ISP vs. over-the-top media (browser or app)
- Distributed vs. concentrated
- Local vs. remote
- Trust your local ISP vs. trust remote browser vendor?
- User choice vs. application’s choice
  - You won’t even notice

Questions

mir@ripe.net
@mir_ripe_labs