Internet Society

# The IETF Ornithology

A Currated Overview of Public Policy Aspects in IETF Work

Olaf Kolkman (editor)

## Contents

## Introduction

This document serves as an aid for people who are observing the work in the Internet Engineering Task Force (IETF) from a policy-based perspective. We have try to indicate which activities might be of policy interest.

This is not the only curated list for people with other than technical interest of IETF activity. Article 19 produced a web page with an overview of working groups whose work that has human right considerations. Also, the IETF itself publishes lists of new topics at IETF meetings e.g. for IETF 119. This curration may have some overlap with others. Completeness is neither claimed nor guaranteed.

Earlier we published a word document with the ornithology. We are now experimenting with a github based curration that is easil compiled into a web page or a pdf document and, more importantly, allows for github based collaboration.

This version of the Ornithology has been last updated for IETF 119.

# 1 The IETF

The IETF work is organized in working groups that are themselves clustered in areas. There are currently 7 areas.

- Internet Area (int) - dealing with IP packets and how to Internetwork
- Routing Area (rtg) - about how to route those packets.
- Web and Internet Transport (wit) - provides abstract end to end connections for applications to use.
- Operations and Management Area (ops) - works on managing and operating IP based networks
- Applications and Real-Time Area (art) - provides building blocks for applications
- Security Area (sec) - provides security building blocks for it all.
- General Area (gen) - is about organizing the IETF and it s governance.

The descriptions above are quite informal, more information about Areas can be found on the IETF Areas webpage

## 1.1 Birds of a Feather (BOFs)

In general, BOFs (Bird of a Feather[1] ) meetings are interesting because they discuss potential new streams of work. It is the place where new work often surfaces. Information on BOFs can be found on the IETF data tracker.

At IETF 119 we find the following BOFs. We have supplemented this with a high-level summary and relation to what might be policy interests. Readers are advised to follow the link in the title to gather more background about the BOF and find links to related Internet drafts and other prior art.

Often, before working groups are formed, meetings are organized to assess if there is enough clarity and interest around a particular issue to form a working group.

At IETF119 we identified the following BOFs that may be of interest.

### 1.1.1 Workload Identity in Multi System Environments (wimse)

- bof request
- Keywords: Identity, cloud service

[1] From From “Birds of a feather flock together” an English proverb, also the inspiration for the esoteric title of this document.

Currently, identification of workloads that provide services and identification of humans in interaction with services are done using two different protocols (SPIFFEE and OAUTH respectively). The communities associated with these have identified common challenges.

This BOF about forming a working group to identify, articulate, and bridge the gaps and ambiguities in workload identity problems and define solutions across a diverse set of platforms and deployments, building on various protocols used in workload environments.

This work may have aspects related to platform interoperability.

### 1.1.2 New DNS Delegations (deleg)

- Bof request
- Keywords: DNS, core infrastructure, confidentiality

  Within the DNS protocol the NS and DS records are used to signal to clients (resolvers) how the authority to serve and sign information within a specific part of the DNS is delegated. Within the DNS ops working group, there is a need to securely signal new technical capabilities such as the availability of authentication, confidentiality, and/or more efficient transport mechanism. This BoF will help people outside the DNS ecosystem understand how this new form of delegation might affect their use of the DNS. It will be an opportunity to hear already-proposed delegation capabilities as well as to brainstorm on new capabilities.

### 1.1.3 Secure Patterns for Internet CrEdentials (spice)

- Bof request
- Keywords: identity, credential, verification, digital public infrastructure

Digital credentials based on IETF standards (and standards in other SDOs) have use cases ranging from individual credentials, such as driver's licenses, age-verification, and vaccination proofs, to business-to-business or business-to-government application. One example is fraud and counterfeiting prevention in cross-border trade documents by protecting digital representations of mill test reports, bills of materials, bills of lading, or commercial invoices. In order to meet privacy, security, and sustainability objectives, digital credentials need to be designed with awareness of computation and storage constraints associated with their use cases.

SPICE aims to document digital credential formats based on existing IETF standards, and extend them to support stakeholders that are building compliance and automation systems based on industry adopted ryptography and protocols.

### 1.1.4 Securely COmmunicating NEtwork PROperties(scone pro)

### 1.1.5 Detecting Unwanted Location Trackers (dust)

- Bof request
- Keywords: privacy, personal safety

Location-tracking accessories provide numerous benefits to users (such as being able to figure out where they left their keys this time!), but they can also have security and privacy implications if used to track other individuals without their knowledge or consent.

A community of stakeholders is seeking input from the IETF around the technical requirements and best practices to allow tracker manufacturers to build location-tracking accessories that will be compatible with unwanted tracking detection and alerts on mobile platforms.

This work is a continuation of a discussion at IETF117 and IETF118.

### 1.1.6 SRv6 Operations (srv6ops)

SRv6 is a segment routing technique based on IPv6. Source routing is typically deployed inside provider networks. It is typically used in 5g networks to provide slices with specific service quality. This BOF intends to form a working group to discuss operational practices and deployment approaches.

## 1.2 General Area

## 1.3 Applications and Real-Time Area

### 1.3.1 More Instant Messaging Interoperability (mimi)

- MIMI
- Keywords: messaging, Digital Market Act, interoperability

Defines interoperability mechanism between messaging platforms. A requirement that comes out of e.g., EU regulation.

### 1.3.2 Registration Protocols Extensions (regext)

- REGEXT

- Keywords: DNS, registration data

  EPP is the protocol used between DNS registrars and registries, this work group works on extending the base protocol with functionality needed across top level domains operations

### 1.3.3 Secure Telephony Identity Revisited (stir)

- STIR
- Keywords: spam, anonymity, telephony.

Specify Internet-based mechanisms that allow verification of the calling party's authorization to use a particular telephone number for an incoming call. Mainly used to prevent unwanted robocalls. This work was initiated on request from the US Federal Communication Commission.

## 1.4 Internet Area

### 1.4.1 MAC Address Device Identification for Network and Application Services (madinas)

- MADINAS
- Keywords: privacy, device identification

Lower-level identifiers, such as the MAC addresses used for WIFI, are being randomized to prevent tracking of users on local area networks, impact applications that depend on the assumption of a stable identifiers. This working group seeks to document best practices that minimizes unintended impact of this randomization.

## 1.5 Operations and Management Area

### 1.5.1 Network Management Operations

- NMOP

This working group focuses on the issues operators may face in managing their network now or in the future. Potentially comparing IETF solutions to those developed in other SDOs. This is a relatively new working group that may surface requirements from the industry.

## 1.6 Security Area

### 1.6.1 Messaging Layer Security (mls)

- MLS

Designs protocol for secure communications between groups (think group chats). This working group is in an advanced state.

### 1.6.2 Post-Quantum Use In Protocols (pquip)

- PQUIP
- Keywords: encryption, confidentiality, quantum resistance.

As quantum computers evolve towards, the risk to encryption protocols we use in today's network protocols grows. A timely transition to quantum safe protocols is required if we want long term confidentially and integrity for the communication today. This group sets out guidance for protocol developers to make that happen.

### 1.6.3 Remote ATtestation ProcedureS

- RATS
- Keywords: supply chain, transitive trust

Discusses mechanisms to attest about the trustworthiness of 3rd party components. Something that may be relevant e.g., in supply chains for (government) services. For instance, securing devices such as tokens for 2-factor authentication – where the manufacturer may not be the entity responsible for authenticating the device once it is deployed.

### 1.6.4 Supply Chain Integrity, Transparency, and Trust (scitt)

- SCITT
- Keywords: supply chain, security

Develops mechanisms to increase accountability and interoperability in software supply chains.

### 1.6.5 Software Updates for Internet of Things (suit)

- SUIT
- Keywords: IoT, security

The ability to securely update things connected to the Internet is an important issue for global cybersecurity. This working group creates solutions associated with updating devices that are small, might be hardly ever connected, long lived, and have low storage and battery life. The work in this working group is in advanced stages.

## 1.7 Web and Internet Transport

### 1.7.1 Multiplexed Application Substrate over QUIC Encryption (masque)

- MASQUE
- Keywords: privacy, encryption

Proxies are an established mechanism to tunnel traffic across the network (VPNs being an example). This working group specifies a proxying mechanism based on the relatively new QUIC transport protocol.

# 2 The IRTF

## 2.1 Research Groups

### 2.1.1 Crypto Forum (cfrc)

- CFRG

  Although highly technical, the cfrg is the place where almost all cryptographic building blocks that are used in IETF protocols are evaluated. The open and peer reviewed nature of this work is critical for the security across the Internet – as such the existence of the group is of policy interest.

### 2.1.2 Global Access to the Internet for All(gaia)

- GAIA

Assesses means to bridge the digital connectivity divide.

### 2.1.3 Decentralization of the Internet Research Group(dinrg

- DINRG

Aims to provide for the research and engineering community, both an open forum to discuss the Internet centralization phenomena and associated potential threats, and a platform to facilitate the coordination of efforts in identifying the causes of observed consolidations and the mitigation thereof.

### 2.1.4 Research and Analysis of Standard-Setting Processes Proposed Research Group(rasprg)

- RASPRG

The RASPRG aims to bring together researchers, practitioners, policy makers, standards users, and standards developers to study standardization processes across SDOs, with a particular focus on Internet standard-setting in the IETF. The research is aimed at informing the comprehension of standardization processes and policies, and possibly providing tools and insight.

### 2.1.5 Quantum Internet Research Group(qirg)

# 3 The IAB

These present a high-level view of the situation in the organization.

# 4 During a meeting

At IETF meeting a number of meetings take place that are of general interest

The IETF plenary is where general administrative reporting takes place and where discussions are being held that are important to the whole community, e.g., about how the IETF governs itself.

The IAB Open Meeting is where the Internet Architecture board presents what it is doing. Usually, it includes discussions of topics about the Internet Architecture and an update on liaisons. The latter is interesting as it provides an insight as to how the IETF relates to other SDOs and technical bodies.

The Internet Research Task Force (IRTF) Open Meeting is where research topics are presented and progress in research groups is reported, it also features presentations of the Applied Networking Research Prize (ANRP) winners.

The Internet Engineering Protocol Group (IEPG), a meeting usually taking place on Sunday, features somewhat more operational presentations of "topical interest". The presentations are technical but usually give an indication about the topics that are interesting to the Internet technical infrastructure's operational community.

Further, the Tutorial: New Participants' Overview is relevant for newcommers while during the Hot RFC session participants try to pitch their documents to make sure interested parties join sessions later in the week.

Finally, the Technology Deep Dive is a mini masterclass for the technical IETF audience on a specific topic.

## About this document

The source for this document can be found on gitub.com/kolkman/ornithology. Readers are encouraged to contribute.