IETF 115 HotRFC

Brought to you by
Spencer Dawkins and **Alexa Morris**

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

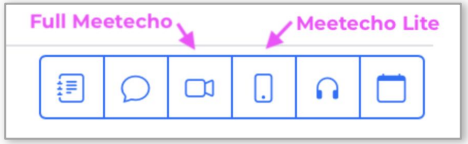
IETF

This session is being recorded

IETF 115 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*
- **Wear masks unless actively speaking at the microphone.**



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Resources for IETF 115 London

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/115/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

The Ground Rules

- **HotRFC is how you make a Request For Conversation**
  - It's a good way to find IETF people to talk to, for various reasons
- Each person gets four minutes from "Go" to "Please Applaud"
  - At four minutes, we start applauding (see next slide)
  - When you hear applause, please hand the microphone over 😇
- We don't do questions here - each person provides follow-up info
  - (in-person attendees can follow presenters to the bar, of course)
- So you can follow along, we're using the datatracker for all slides
  - Let the conversations begin!

Please Applaud!!! (and the crowd goes wild)

COMPUTERATE SPECIFYING

THE FIVE LEVELS OF I-D WRITING

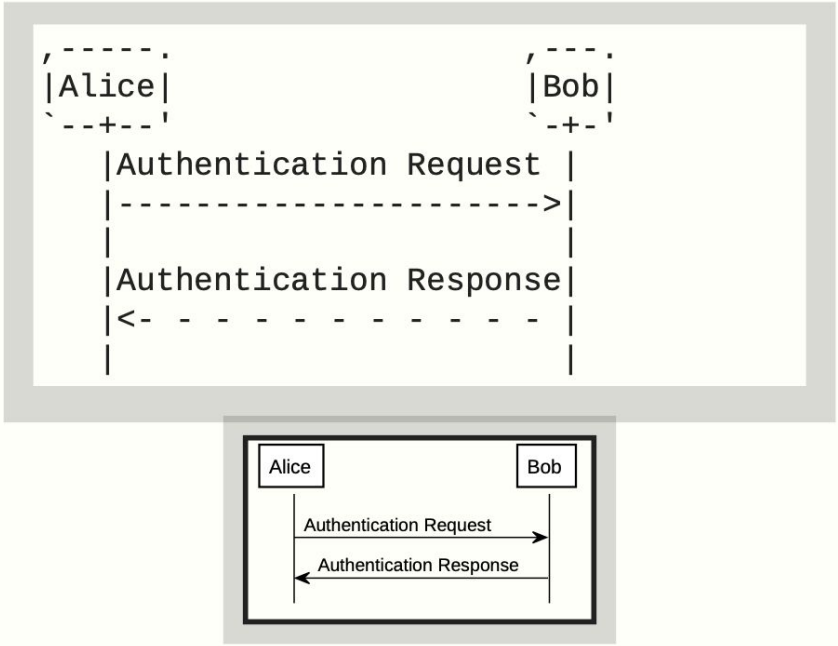
IETF 115 - London UK

Marc Petit-Huguenin

Marc will not be with us tonight.

OLD SCHOOL

A long time ago Internet-Drafts were written directly as text. PDF files had to be designed separately to support graphics.



XML2RFC V3

Nowadays I-Ds are written in XML2RFC v3, which permits to generate text, HTML, and PDF from one source.

```
<artset>
  <artwork type="svg" src="auth.svg">
  <artwork type="ascii-art"><![CDATA[
,-----.                    ,---.
|Alice|                    |Bob|
`--+--'                    `-+-'
   |Authentication Request  |
   |----------------------->|
   |                        |
   |Authentication Response |
   |<- - - - - - - - - - -  |
   |                        |
]]></artwork>
</artset>
```

NEW: ASCIIDOC

AsciiDoc makes it easier to write specifications and can be extended, e.g., to render diagrams.

```
[alt]
====
[plantuml,target=svg]
----
hide footbox
Alice -> Bob: Authentication Request
Bob --> Alice: Authentication Response
----

[plantuml,target=txt]
----
hide footbox
Alice -> Bob: Authentication Request
Bob --> Alice: Authentication Response
----
```

NEW: BASIC COMPUTERATE SPECIFICATION

Computerate Specifying provides the ability of generating some parts of a document from code,

```
> msc : Either (List1 Content)
>   (List1 Block)
> msc = Right (MkAlt (MkPlantUml Nothing
>   Svg """
> hide footbox
> Alice -> Bob: Authentication Request
> Bob --> Alice: Authentication Response
> """ ::: [MkPlantUml Nothing Txt """
> hide footbox
> Alice -> Bob: Authentication Request
> Bob --> Alice: Authentication Response
> """]))

code::[msc]
```

NEW: ADVANCED COMPUTERATE SPECIFICATION

and ad-hoc polymorphism can be used to convert an Idris type into AsciiDoc.

```
> msc : PlantUml
> msc = do
>   hide footbox
>   alice <- actor "Alice"
>   bob <- actor "Bob"
>   arrow alice bob """
> Authentication Request
> """
>   dotted-arrow bob alice """
> Authentication Response
> """

code::[msc]
```

FOLLOW-UP

- Hackdemo Happy Hour Monday 18:00 - 19:00 in Admiral 1
- https://datatracker.ietf.org/doc/draft-petithuguenin-xml2rfc-asciidoc/
- https://datatracker.ietf.org/doc/draft-petithuguenin-computerate-specifying/
- Marc Petit-Huguenin <marc@petit-huguenin.org>

Please Applaud!!! (and the crowd goes wild)

The Mesh
The Multiverse
and EVERYTHING

Phill Hallam-Baker

In case you missed it

MATHEMATICAL MESH

End-to-end security takes time:

“If you want to deliver an end-to-end secure app in 2023, best start in 2018”

MATHEMATICAL MESH

The Mesh is designed to support

- End-to-end secure private key management
- End-to-end secure data at rest
- End-to-end secure messaging, email, sharing of large files
- End-to-end secure chat, voice, video

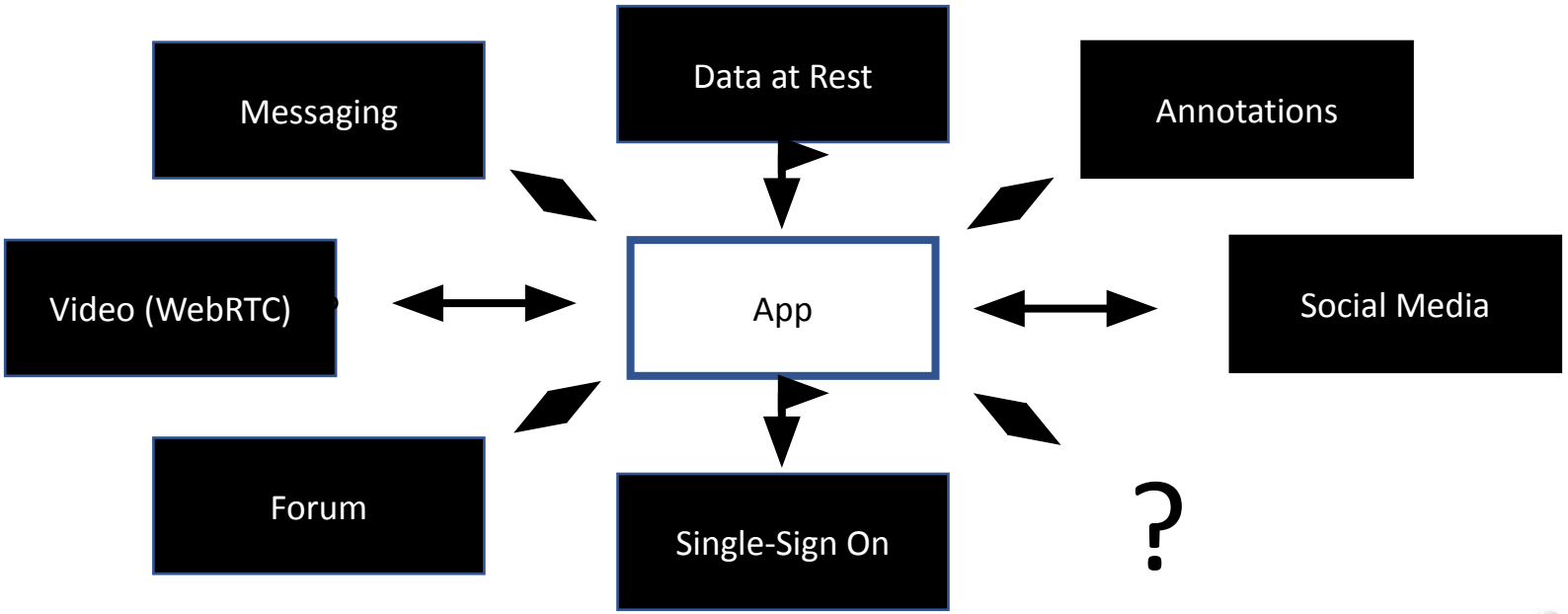
MATHEMATICAL
MESH

The Mesh is designed to support

- End-to-end secure private key management
- End-to-end secure data at rest
- End-to-end secure messaging, email, sharing of large files
- End-to-end secure chat, voice, video
- **End-to-end secure small group collaboration**
- **End-to-end secure large group collaboration**
- **End-to-end secure social media**

MATHEMATICAL MESH

A complete communications infrastructure



MATHEMATICAL MESH

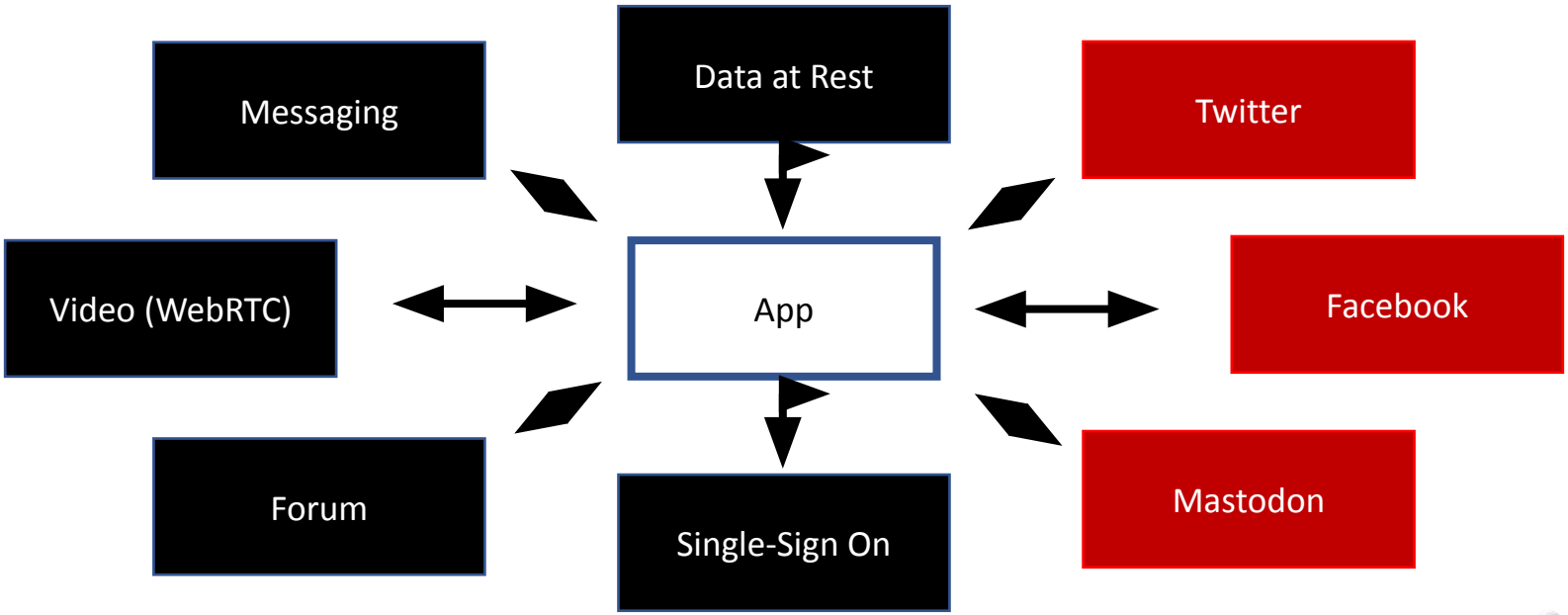
So why not build an Open Social Media?

- Accounts belong to users, not their service provider
- Users choose their service provider, can change at any time
- Users choose curators providing feeds that meet their needs

- A multiverse of all points of view

MATHEMATICAL
MESH

Hang on, what about Mastodon?



MATHEMATICAL MESH

What to call it?

Everything

Mathmesh.com

https://www.ietf.org/archive/id/draft-hallambaker-everything-00.html

Please Applaud!!! (and the crowd goes wild)

KIRA – Scalable ID-based Routing Architecture for Control Planes

Karlsruhe Institute of Technology

- Goals: 1st connectivity, 2nd route efficiency → highly resilient control plane
- Scalability: 100,000s of nodes (in a single domain)
- Routes on NodeIDs (no ID → locator mapping)
- Routing Table:
  - Size: $O(\log n)$ entries [NodeID → <Path Vector>], shortest paths
  - Per-node selectable memory/stretch trade-off
- Zero-touch: no configuration required
- Topological versatility: works well in various topologies
- Loop-free (even during convergence)
- Uses PathIDs as labels in its forwarding tier
- Provides zero-conf IPv6 connectivity

KIRA: Kademlia-directed ID-based Routing Architecture

KIRA – What else? Where can I get more info?

- Special end-systems mode → reduces overhead even more
- Supports multi-path routing and forwarding
- Built-in DHT, e.g., for name or service lookups / discovery
- KeLLy – Scalable, efficient topology discovery based on KIRA

KIRA provides highly scalable, resilient, zero-conf control plane connectivity

More information on KIRA:

- Scheduled presentations @IETF115
  - RTGWG Thursday (Nov 10th), 13.45h
  - ANIMA WG Thursday (Nov 10th), 14.30h

Contact: bless@kit.edu

Paper:

https://s.kit.edu/kira

Please Applaud!!! (and the crowd goes wild)

Mobile User Plane Evolution

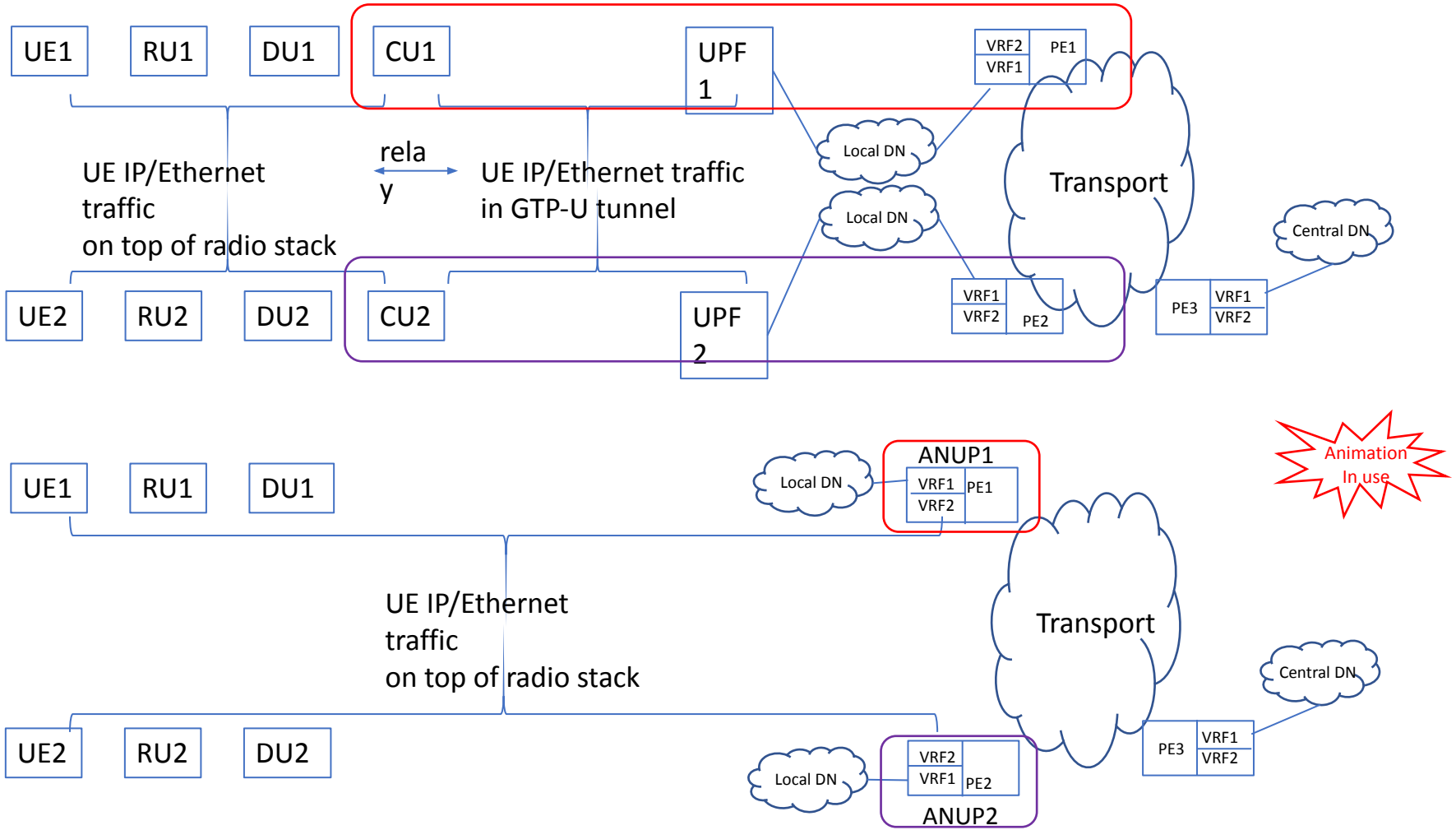
draft-zzhang-dmm-mup-evolution-02

Jeffrey Zhang, Keyur Patel, Luis Contreras, Kashif Islam

IETF 115, HotRFC

5G User Plane

- Mobile Communication Network (MCN): RAN + CN
  - Radio Access Network (RAN)
    - A network of radio access components (gNB) that terminate the air interface from UEs
    - Decomposed RAN with RU/DU/CU split
  - Core Network (CN)
    - The brain of an MCN; to enable and implement mobile services
- User Plane: data plane that carries mobile user traffic
  - Spans from UE to RU/DU/CU (RAN) to UPF (CN)
  - User Plane Function (UPF) is a NF in CN – like a BNG
    - Routing/switching between UE and the Data Network (DN) – SDN style
- Distributed UPFs co-located with CUs
  - For MEC, private 5G, and local Internet peering
  - Requires distributed DN – implemented as VPN (DNVPN)

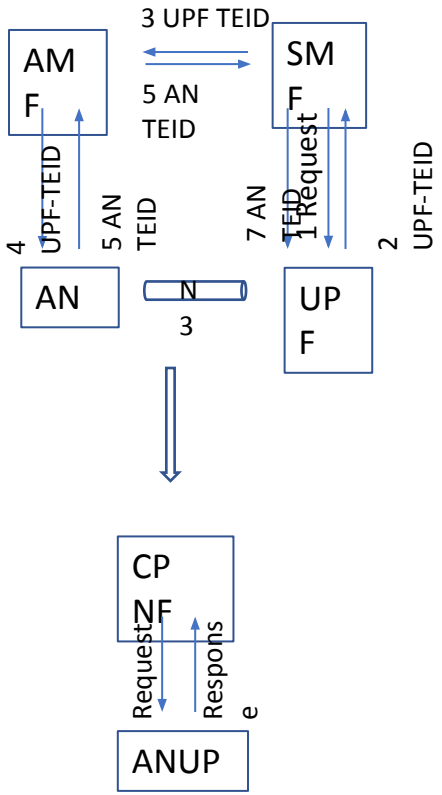

UE1
RU1
DU1
CU1
UPF 1
VRF2
VRF1
PE1
Local DN
Transport
Central DN
UE IP/Ethernet traffic
on top of radio stack
rela y
UE IP/Ethernet traffic
in GTP-U tunnel
Local DN
UE2
RU2
DU2
CU2
UPF 2
VRF1
VRF2
PE2
PE3
VRF1
VRF2
Animation
In use
ANUP1
Local DN
VRF1
VRF2
PE1
UE1
RU1
DU1
Transport
Central DN
UE IP/Ethernet
traffic
on top of radio stack
UE2
RU2
DU2
Local DN
VRF2
VRF1
PE2
ANUP2
PE3
VRF1
VRF2

Integrating gNB-CU and UPF

- ANUP: AN (gNB-CU) and UPF functions integrated into a single NF
  - Optionally with DNVPN PE function integrated
  - Integration when desired/feasible, separation when required
- A router/switch with wireless/wired connections
  - 3GPP/wireless technologies for wireless access, just like:
    - IEEE technologies for Ethernet connection to a router
    - WIFI technologies for WIFI connection to a router
  - IETF/IEEE/wireline technologies for the rest:
    - Routing/switching
    - VPN/EVPN/whatever features/services as currently in wireline world

Advantages

- Simplified signaling and optimized data plane
  - No more N3 (GTP-U) tunneling
    - The need for N3 tunneling was due to central UPFs
  - 7-step signaling involving 4 NFs and 3 interfaces reduced to 2-step signaling
- Unified architecture for wireline/wireless
  - A router/switch with wireless/wired connections
  - Many 5G special features/procedures are not needed anymore or can be greatly simplified
    - MEC, 5MBS, LAN-type services, etc.



Will 3GPP Accept Integrated ANUP?

- It seems a natural evolution
  - To people familiar/friendly with IETF/wireline technologies
  - But a big paradigm shift on 3GPP/wireless side
- But the work is to be done in 3GPP
- Trying to get support from mobile operators
  - Socializing the idea first among their IETF/wireline people on mobile side
- Will bring to 3GPP if we get enough support
  - The work is on 3GPP not IETF side

Please Applaud!!! (and the crowd goes wild)

Supercharging Traceroute

Valentin Heinrich
Rolf Winter

Hochschule
Augsburg University of
Applied Sciences

State of the network or when sth. goes wrong…

- The IETF has defined an extensive set of OAM machinery, e.g.
  - YANG/Netconf/Restconf:
    Let's you monitor (and configure) everything related to **your** boxes
  - In Situ OAM (IOAM):
    Let's you measure everything related to **your** segment of a path
  - IPFIX, …
- What about the public internet?
  - Ping: interface reachability and RTT
  - Traceroute: router-level path **towards** a destination and RTT to each hop

We would like to make traceroute better, by also measuring the reverse path

*source: yangcatalog.org

Join the discussion, help us measure and improve

- Read the draft and join the discussion (well, start really) at INTArea
- Offer to host a reverse traceroute end-point
- Use our reverse traceroute client and send us the output
- Remember, the internet is for end users (RFC 8890), so is this work
  - People and organizations running infrastructure in the cloud
  - People and organizations consuming services over the public internet
  - ...
- Website: https://net.hs-augsburg.de/en/project/reverse-traceroute/
- Github: https://github.com/HSAnet/reverse-traceroute
- Contact: rolf.winter@hs-augsburg.de

https://datatracker.ietf.org/doc/html/draft-heiwin-intarea-reverse-traceroute

Please Applaud!!! (and the crowd goes wild)

Encrypted Client Hello Deployment Considerations

Andrew Campling Andrew.Campling@419.Consulting

Arnaud Taddei Arnaud.Taddei@broadcom.com

Simon Edwards Simon.Edwards@broadcom.com

Paul Vixie Paul@Redbarn.Org

David Wright David.Wright@SWGfL.Org.UK

Context

- Encrypted Client Hello (ECH) is “a mechanism in Transport Layer Security (TLS) for encrypting a ClientHello message under a server public key”
- Builds on the previous Encrypted Server Name Indication (eSNI) proposal
- Being developed within the IETF’s TLS working group
- See https://datatracker.ietf.org/doc/draft-ietf-tls-esni/ for the latest version (currently draft -15)

What is the Issue?

- RFC 7258: discusses the critical need to protect users' privacy when developing IETF specifications, recognises that making networks unmanageable to mitigate pervasive monitoring is not an acceptable outcome.
- RFC 8404 [RFC8404] discusses current security and network operations as well as management practices that may be impacted by the shift to increased use of encryption.

  "The implications for enterprises that own the data on their networks or that have explicit agreements that permit the monitoring of user traffic are very different from those for service providers…"

- The data encapsulated by ECH is of legitimate interest to on-path security actors including anti-virus software, parental controls [and other content filtering] and consumer and enterprise firewalls.

RFC 8744 – “Issues and Requirements for Server Name Identification (SNI) Encryption in TLS”

- Includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1)
- A brief (two paragraph) assessment of alternative options in the event that the SNI data is encrypted (section 2.3)
- Asserts, with limited evidence, that "most of [the unanticipated usage] functions can, however, be realized by other means“
- Does not consider or quantify the affordability, operational complexity or technical capability of affected parties or the privacy implications that might be involved

If This Interests You….

- Draft currently in development that documents the operational impact of ECH for various use cases
  - https://datatracker.ietf.org/doc/draft-campling-ech-deployment-considerations/
  - To be updated with an -03 version shortly
- Side meeting tomorrow evening to discuss this further
  - When: Monday 7th December, 19:00-20:00 UTC
  - In-Person: Richmond 6
  - Remote: https://us02web.zoom.us/j/84216816172?pwd=R0Y5NHEwenNYTjZmUWJnL29lSE5LUT09&from=addon

Thank You

Andrew.Campling@419.Consulting

Please Applaud!!! (and the crowd goes wild)

The JSON format for vCon Conversation Data Container

Dan Petrie, SIPez
Thomas McCarthy-Howe, Strolid

What's a conversation? And what's in THAT conversation?

- Data generated in communications systems is siloed, opaque and exported in proprietary formats, if it's exported at all.
- Conversations have many modes: messaging, video, voice (meta?), and customers use more than one mode all the time. Not a single standard to capture omni-channel customer journeys.
- Customer facing organizations record conversations, for very good operational, marketing and sales reasons, for the benefit of the shareholders and customers.
- Responsible organizations should treat customer data with the same care as organizational data.
- GDPR, CCDPA and similar legislation world-wide demand the right of a person to be forgotten by a business, to remove that data from the business, to be as if the relationship between them never existed.
- How do you keep track of what customer biometric data was used in AI training? Changing your name is way easier than changing your face or your voice

The vCon Standard in Four Parts

Dialogs

Timestamped recordings of conversations, chat transcripts, video recordings. Can be from a single mode or many. Can be packed or external (URL)

Parties

Identification and location of the parties in the dialogs, including the authenticating organization or method, such as STIR PASSPORT

Analysis

A series of third party analysis of the conversations: sentiment :) :(, quality (MOS), agent compliance, transcriptions, translations, redactions, data labels

Attachments

Documents that provide the context of the conversation: PowerPoint, Sales Leads, NDAs

Practical Problems We Are Solving

- Allows us to responsibly share conversations with stakeholders
- Standardizing the format enables an ecosystem of tools and reference sources
- Removes siloed data and enables people to move between service providers and communications systems without losing this data
- Enables data engineering for conversations to support ML and AI (Robot Food)
- Enables strong authentication and identification of parties in conversations to reduce fraud
- General Conversation Management: signing and verification, encryption, content redaction, data packing / unpacking, appending to a signed document, grouping of vCons together in a set

More information

Learn more at:

- **Mailing List**: https://www.ietf.org/mailman/listinfo/Vcon
- **I-D:** https://datatracker.ietf.org/doc/draft-petrie-vcon/
- **Open Source**: https://github.com/vcon-dev/vcon
- **White Paper**: https://bit.ly/vcon-wp

IETF 115:

- **Hackathon:** Saturday and Sunday
- **HotRFC**: 18:00 Sunday
- **ART dispatch WG meeting:** Mon 9:30
- **Hackathon Happy Hour**: Mon 18:00 Admiral 1
- **vCon Bar BoF**: Thurs. 15:30-16:30 Richmond 6

Please Applaud!!! (and the crowd goes wild)

Encrypted Transport over Satellite

ETоSat @ IETF 115

Encrypted Transport over Satellite

- EToSat is a non-working group mailing list used to discuss topics related to carrying IP traffic over Geostationary (GEO), Medium Earth Orbit (MEO) and Low Earth Orbit (LEO) satellites
  - List was started to discuss the use of encrypted transport protocols (e.g. QUIC) blocking traditional GEO satellite solutions such as Performance Enhancing Proxies
    - Hence the name
  - Has expanded to include other satellite Internet access topics including, for example, dealing with frequent connectivity changes when using LEO constellations

- Mailing list: etosat@ietf.org
- To subscribe: https://www.ietf.org/mailman/listinfo/etosat

EToSat Side Meeting

- A side meeting is scheduled to discuss some GEO-specific topics
  - The currently scheduled presentations are:
    - Very Brief EToSat Introduction
      - John Border, Hughes
    - Transport for High BDP Networks
      - Jae Won Chung, Viasat
    - QUIC and FEC
      - François Michel, UCLouvain, Belgium
    - Reducing the acknowledgement frequency in IETF QUIC
      - Ana Custura, University of Aberdeen
    - Suitability of BBR for QUIC over GEO

      Aitor Martin or Naeem Khademi, University of Stavanger, Norway

EToSat Side Meeting

- Wednesday, November 9, 11:45 to 12:45 in Richmond 6
  - Remote participation also supported

- For more information…
  - John Border (John.Border@Hughes.com)
  - EToSat mailing list (etosat@ietf.org)

Please Applaud!!! (and the crowd goes wild)

Can formal specifications help?

Lenore Zuck (University of Illinois Chicago)
Ken McMillan (University of Texas at Austin)

Some uses of formal specifications

- Unambiguous documentation for users and implementers
  - Interface contract
- Conformance testing
  - Run-time monitoring
  - Automatic test case generation
- Formal proof of correctness properties
  - Even without formal proofs, formal specifications are very useful!

Example: Specification of QUIC

- Formal wire specification of (a subset of) QUIC
  - Detailed enough to execute the protocol and interact with implementations
  - Automatically tested compliance four server implementations with the spec
- Discovered numerous errors caused by:
  - Misinterpretation of the RFC's
  - Ambiguities in the RFC's
  - Low-level coding errors
- Some were exploitable!
  - For example, client can read uninitialized memory of server

Takeaways

- Interoperability testing is not enough
  - Misses compliance failures
  - Leads to ossification and future security issues (e.g. SSL)
- Formal specification can be a solution
  - Allows us to detect compliance failures early
- There are hard trade-offs between uses
  - Readability *vs* testing *vs* formal proof
  - More work is needed!

We would like to understand how to integrate formal specifications into the IEFTF process. If you're interested in this topic, please join us at the side meeting of the Usable Formal Methods Research Group!

Please Applaud!!! (and the crowd goes wild)

The problem of mass unauthorized security scans/tests

Presenter: Rich Kulawiec, Fire on the Mountain (remote) Contact: rsk@firemountain.net

Introduction:

An increasing number of operations are conducting mass security scanning/testing of as many systems as they can. This trips alarms, fills logs, consumes human time, is being done without permission, builds datasets that are highly useful to attackers who can't build their own, and won't scale.

Goal:

Discussion. Do we concur that this is a problem, and if so, do we think it's a problem we can/should address, and if so, then what can we do (RFC? BCP?) to address it? I suggest a temporary mailing list to ask/answer these questions.

The problem of mass unauthorized security scans/tests

Notes:

1. I estimate 30+ such operations so far but I'm probably undercounting. I've observed ~4000 (IPv4) originating addresses, also likely an undercount.

2. These aren't the preludes to attacks, they ARE attacks. These are active probes of services (e.g., SSH, IMAP), not passive data gathering.

3. Dealing with these attacks costs time/money/effort on the part of the targets. Note that identifying and blocking these is at best onerous, reactive, and only partially effective.

4. Some operations have gone to considerable lengths to obfuscate their identities and activities, e.g., frequently shifting origination points.

5. Aggregating this kind of data builds a valuable target. (Other) attackers will want it, and they'll get it. This makes the entire Internet *less* safe.

The problem of mass unauthorized security scans/tests

Notes, continued:

6. They're not (all) researchers. Consider:

- Have they fully identified themselves, the purpose of the research, its goals, its methods, its scope, etc.?
- Have they put their research proposal in front of an IRB?
- Did they get the informed consent of the subjects of their research before commencing?
- Did they provide the results of tests to the subjects?
- Have they published?

The problem of mass unauthorized security scans/tests

So, looping back to the beginning:

- Do we concur that this is a problem?
- If so, do we think it's a problem we can/should address?
- If so, then what can we do (RFC? BCP?) to address it?

I suggest a temporary mailing list to ask/answer these questions.
Thanks, and comments/questions/etc. to: Rich Kulawiec, rsk@firemountain.net.

Please Applaud!!! (and the crowd goes wild)

SIP-over-QUIC

IETF 115 HotRFC talk

06 NOV 2022

Sam Hurst

BBC RESEARCH & DEVELOPMENT

SIP-over-QUIC
Context

- A mapping of **Session Initiation Protocol** (SIP) semantics over **QUIC Transport**
- Design inspired by **HTTP/3**
- Original idea was born from work on my QUIC RTP Tunnelling draft
  - draft-hurst-quic-rtp-tunnelling
- Sending live media over QUIC is an active topic, including the new Media-over-QUIC (**MoQ**) WG.
- Possibility of reusing SIP semantics to convey **control metadata** about media sessions using SIP offer/answer

SIP-over-QUIC
System design

- Design **inspired by HTTP/3** allows potential reuse of lots of existing HTTP/3 stack development
- Intention to allow for media sessions to reuse the QUIC transport connection initiated by a SIP-over-QUIC session to send media in the same encrypted tunnel
  - Deliberately doesn't choose a media transport type to allow for flexibility
- **DATA** frames are compatible with H3
- **HEADERS** frames feature QPACK compression
- Use of both client- and server-initiated bidirectional streams for sending SIP request messages
  - Decouples the UAC and UAS from the QUIC client and server model
- Unidirectional stream types reserved for **media transport**
  - **Datagrams** also available

SIP-over-QUIC
What next?

- Internet-Draft is ready and will be posted as soon as the datatracker is accepting new submissions again
  - Editor's draft available at https://bbc.github.io/draft-hurst-sip-quic/draft-hurst-sip-quic.html
- Happy to accept any and all feedback
- Which working group is the best avenue to continue this work?
  - SIPcore?
  - AVTcore?
  - MoQ?

Thank you for listening

For more information:

E-mail: sam.hurst@bbc.co.uk

Please Applaud!!! (and the crowd goes wild)

Presentation goes here

Quo vadis IETF?
Is the IETF (becoming) ossified?

Ignacio Castro

IETF 115 - HotRFC

Is the IETF “organisationally healthy”?

- More complex discussions
- Harder to publish
- Influential minority

SODESTREAM: Analysing decision making in the IETF

Published work:

- P. Khare, M. Karan, S. McQuistin, C. Perkins, G. Tyson, M. Purver, P. Healey, I. Castro. *"The Web We Weave: Untangling the Social Graph of the IETF".* AAAI ICWSM, 2022.
- S. McQuistin, M. Karan, P. Khare, C. Perkins, G. Tyson, M. Purver, P. Healey, W. Iqbal, J. Qadir, Ignacio Castro. *"Characterising the IETF Through the Lens of RFC Deployment"*. ACM IMC, 2021
- Talk at maprg

Project:

- SODESTREAM: Streamlining Social Decision Making for Improved Internet Standards (https://sodestream.github.io)

Queen Mary University of London

EPSRC Engineering and Physical Sciences Research Council

University of Glasgow

SODESTREAM: Analysing decision making in the IETF

- What tools would help?
  - cross-area review recommender tool

- **Help us!** *Please, please, pleaaaase*
  - Ground-truth & General feedback/insights
  - Survey: reviewer recommender tool

- Join us:
  - RASP RG: Researching Internet Standards Processes Research Group
  - Side meeting: Thurs-10th 3.30pm

Please Applaud!!! (and the crowd goes wild)

TMP: Time Modulation Protocol

Hans-Dieter Hiep <hdh@cwi.nl>


Universiteit Leiden
The Netherlands

Centrum Wiskunde & Informatica

Received funding from:

The big picture

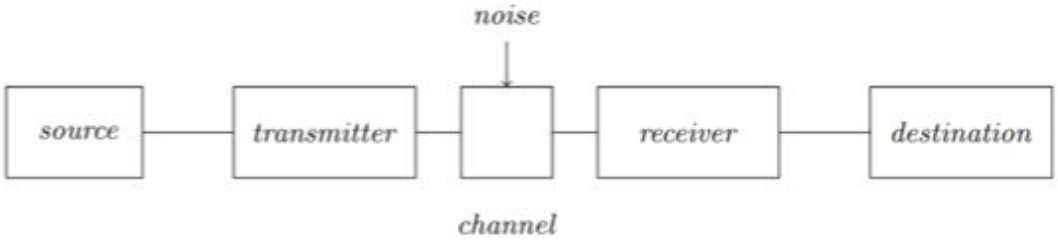


Fig. 1. Diagram representing the different components involved during communication.

- Foundation: Shannon's **Information Theory** (1948)
- Capacity of a channel: **bits/second**
- **Time insensitive** measure

Side channel: time

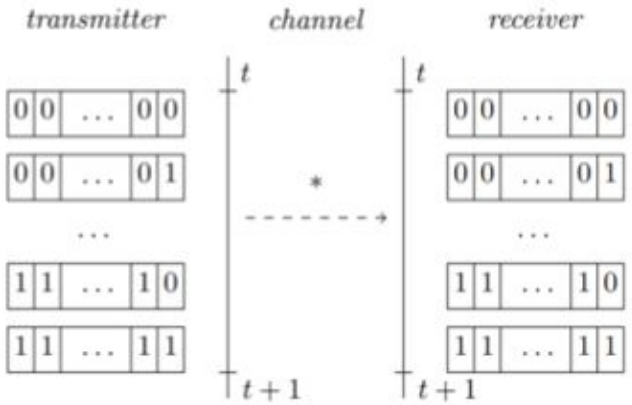


Fig. 4. Alternatively, with a time-sensitive transmitter and receiver, the capacity of a channel is the number of signals that can be sent within a second, and the effective capacity of a transmission system is given by the number of bits that a transmitter and receiver can encode per signal.

- Effective capacity (bits/second)

Theorem. Effective capacity > capacity

- Jitter (seconds): **unpredictable variation in delay**

Time Modulation Protocol

Requirement: **high-precision clocks**

Potential benefits:

- Increase effective capacity
- Increase confidentiality (**hiding data in time**)

Looking to **standardize** new Internet protocol: TMP.

Looking for **collaboration** on:

- Prototype implementations
- Better models for predicting delays

Please Applaud!!! (and the crowd goes wild)

IWF Internet Watch Foundation

IWF @25

Is Privacy Preserving Web Filtering Possible?

Dan Sexton

CTO, Internet Watch Foundation

Search 'Internet Watch Foundation'

The Challenge

The IWF works to find and remove child sexual abuse material from the internet (CSAM). A crucial part of this work has been providing data to industry to enable detection and blocking of verified CSAM by platforms and ISPs.

As internet standards have developed and use of encryption become commonplace, the methods that organisations used to perform legitimate filtering of harmful content have become less and less effective.

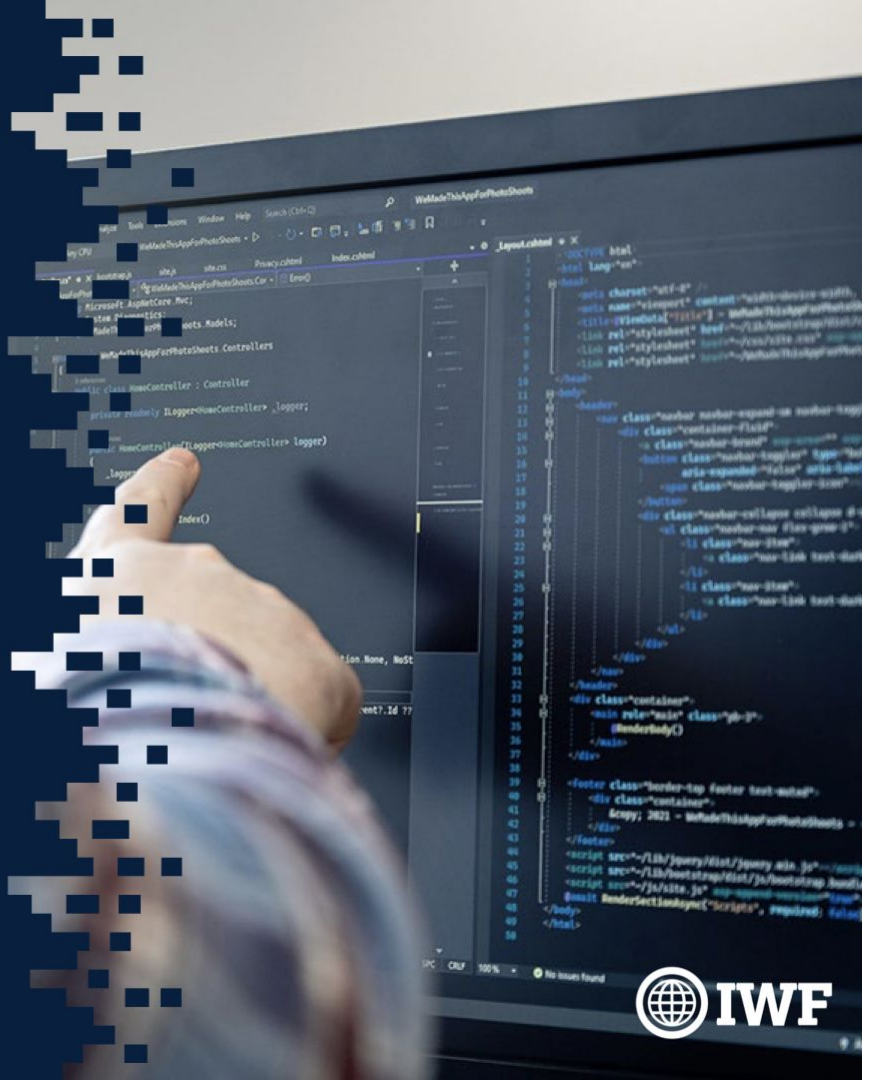
Can legitimate, legal web filtering co-exists with a secure and private internet? Can advances in encryption and privacy enhancing technologies be leveraged to filter harmful web content *without* compromising user privacy?

Searching for Solutions

IWF wants to engage with the community of engineers and tech industry leaders that shape Internet standards to stimulate practical solutions, standards, and/or implementations of web filtering that do not compromise user privacy.

I am looking to find out about any existing work on privacy preserving web filtering, or privacy enhancing uses of technology that could be made to work.

And to otherwise pose an engineering challenge to the IETF attendees that might develop into future proposals, standards or implementations.



Please Applaud!!! (and the crowd goes wild)

Matrix+MIMI

travisr@matrix.org
@travis:t2l.io

The three questions

matrix

1. What is MIMI?
2. Why are we doing this, and how does it affect us?
3. Where are we at?

What is MIMI?

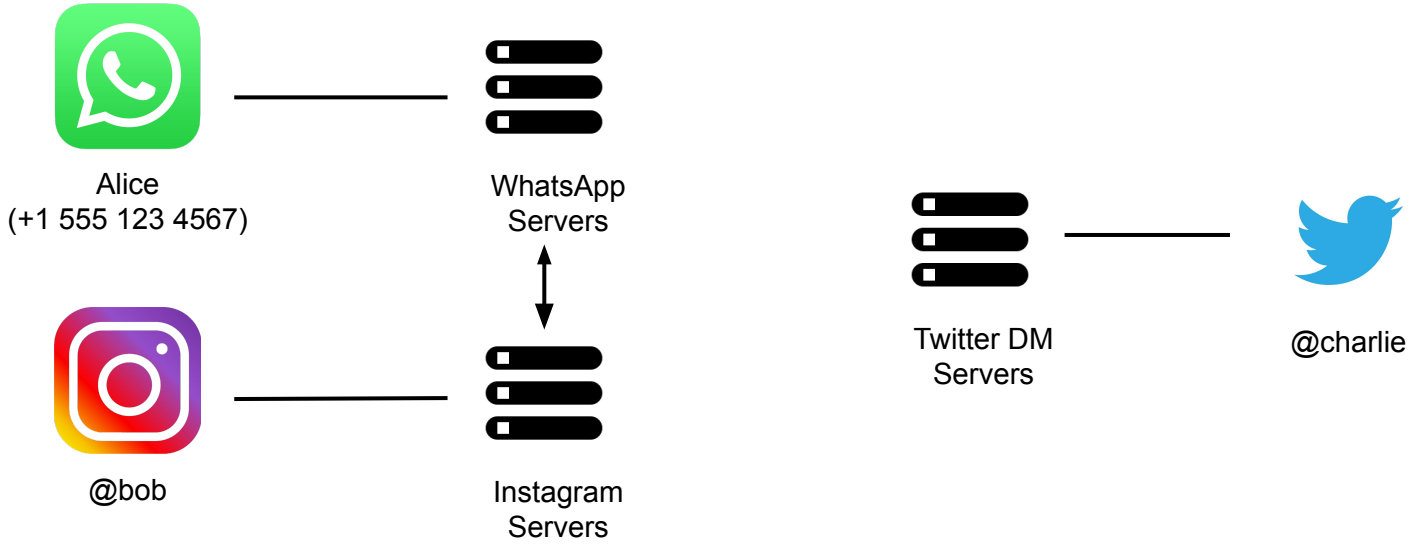
MIMI

matrix

- More Instant Message Interoperability working group at IETF
- Created out of an interest to standardize support for the EU Digital Markets Act (DMA)
- DMA requires “gatekeepers” to interoperate with other messengers
- We think this is a good thing
- Matrix is an interoperable open standard for secure, decentralized, communication
- You might see where this is going…

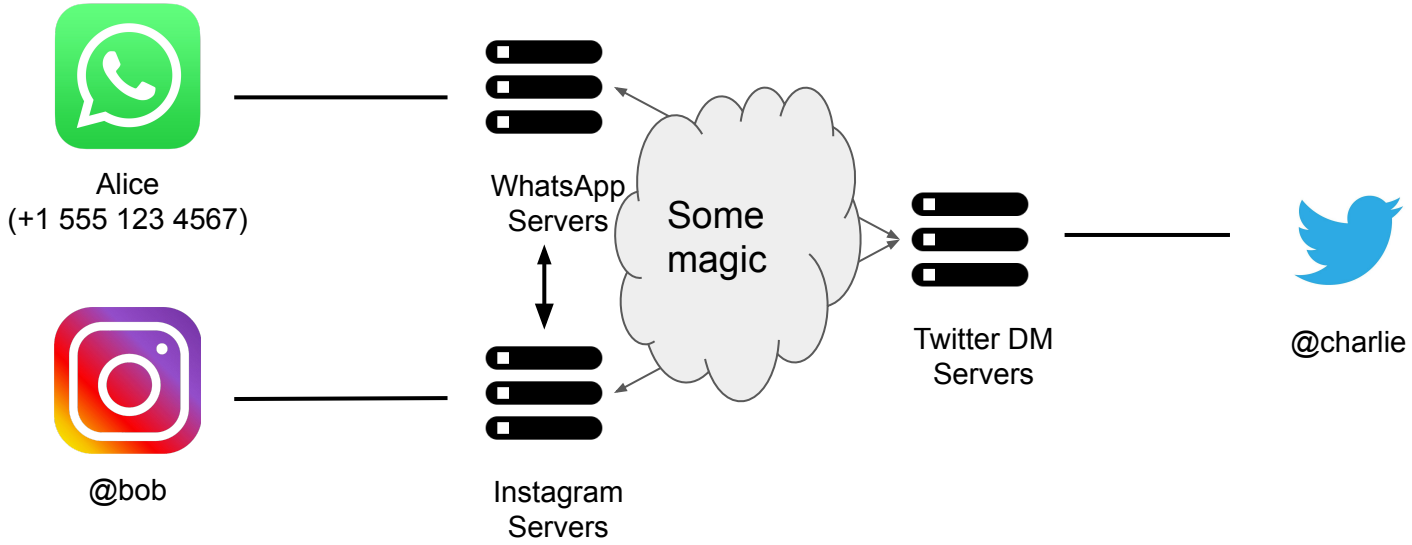
Gatekeepers: Today

matrix

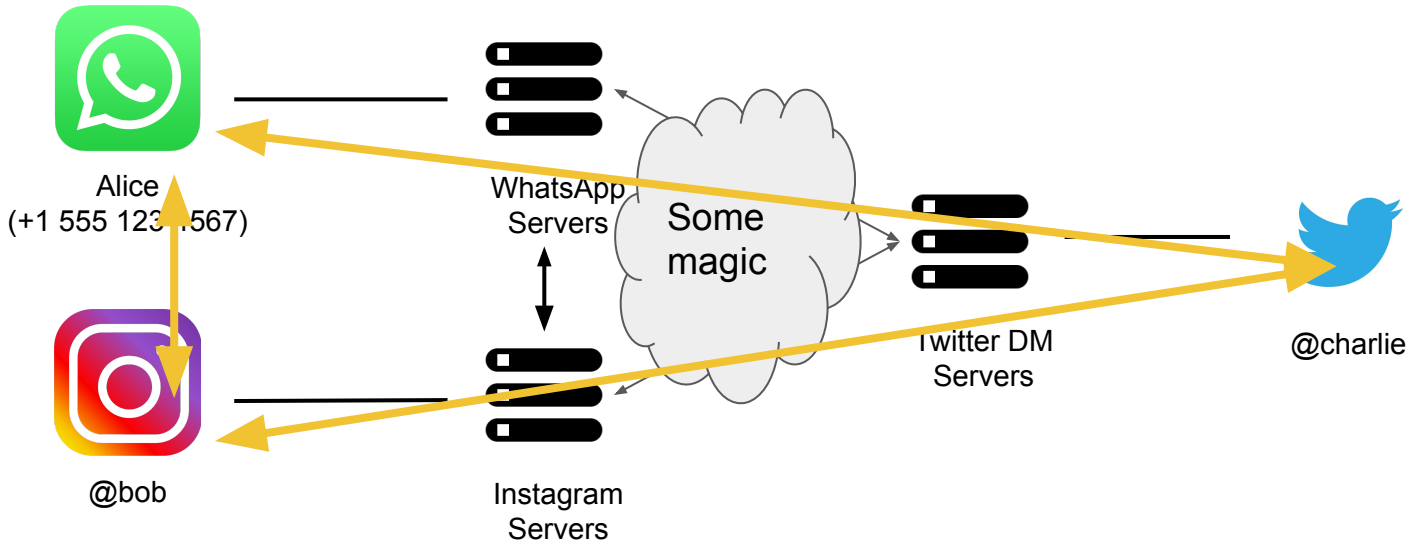


What DMA wants

matrix



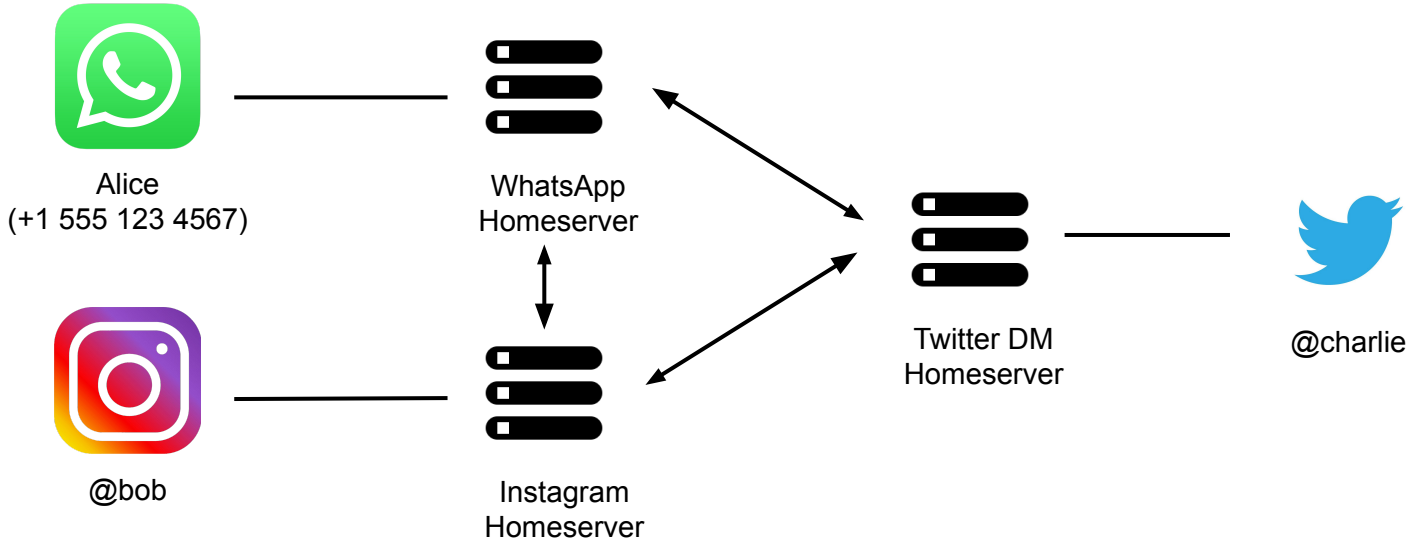
… but also by maintaining E2EE



So, how would we do that?

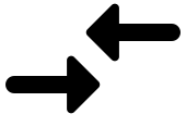
With Matrix, of course

Matrix used for interoperability



The bits we need

matrix



Federation API & HTTPS Transport (MSCs coming soon)

Extensible Events (MSC1767 + friends)

Governance process to maintain an LTS (MSC3923)

Federation API

matrix

- Server to Server Communication layer
- Alternative transports supported, but we're suggesting HTTPS for now
- Algorithms are kept in room versions (just like they are today)
- It doesn't involve any of the Client-Server API
- Implementation is relatively easy as a result
- Gitter case study shows how it could be done quickly

Extensible Events (MSC1767)

matrix

- Events contain information that is sent over the Federation API, like text messages
- Can be end-to-end encrypted using Olm/Megolm or (D)MLS
- Interoperable using “Content Blocks” (alternative representations of complex events)
- We’re not actually proposing any event types to IETF, just the schema
- Matrix.org Foundation (and others) could become “registrars” for event types
- Collections of event types form features, like Instant Messaging, VoIP, 3D Worlds, etc
- Upcoming MSC describes this a bit better than this slide does

Governance (MSC3923)

- We want to maintain rapid prototyping as a feature
- Don’t want to propose every MSC through the IETF process
- Instead, “snapshot” Matrix as an LTS and maintain forwards compatibility
- Any changes on the IETF side get replicated as MSCs
- Relevant MSCs also get turned into IETF proposals
- If designed well enough, either side could reject a proposal and be fine (but this shouldn’t happen very often)
- Spec Core Team (SCT) needs to sign off on this plan

Where are we at?

November 2022: Status

2014: Matrix Created

2019: Exited Beta

Summer 2022: MIMI started

November 2022: MIMI becomes WG

Q1 2023 and onwards: Lots of discussions

TBD: Matrix adopted by IETF

TBD: Matrix implemented everywhere 🚀

How can you help?

Sorry, it was 4 questions all along

Let us know what you think

#matrix-spec:matrix.org is a great place to chat

Thank you

Please Applaud!!! (and the crowd goes wild)

Thank you to the presenters!

And please, Do the Right Thing!!