KIFÜ

A MAGYARORSZÁGI **DIGITALIZÁCIÓ** SZOLGÁLATÁBAN

KIFÜ

WebRTC &
NAT and Firewall Traversal Update

GÉANT STUN/TURN Pilot infrastructure

Mihály Mészáros

2019.10.09.

KIFÜ

Standardization

W3C WebRTC WG update

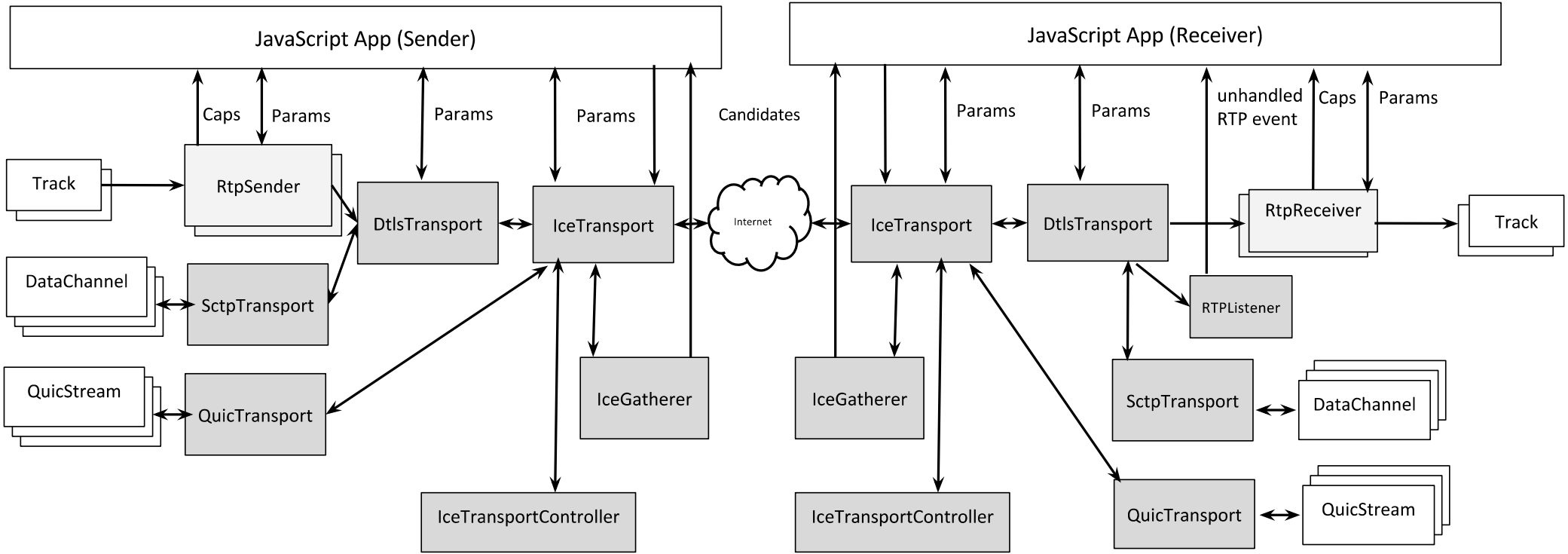
W3C WebRTC Standardization Update

- Finalize 1.0
  - More and more ORTC
- WebRTC-NV moving target
- WG Charis
  - Jan-Ivar Bruaroey (Mozilla)
  - Bernard Aboba (Microsoft)
  - Harald Alvestrand (Google)
- Latest news:
  - https://webrtc.internaut.com/demos/slides/Leveraging_WebRTC.pdf
  - https://www.w3.org/2011/04/webrtc/wiki/September_19-20_2019

~~SDP~~

- Higher Level API
  - Easy to learn, but gives less control
  - Many years discussion (ORTC)
  - Bigger responsibility on the Browser side. (heavy lifting!)
  - To serve all use cases is impossible
    - Even coordinating developments is very difficult
    - Worldwide consensus building is hard question!
- More Detailed API
  - Don’t use SDP anymore, to avoid it’s limitations
  - Less shared media engine code (More flexibility, New use cases!)
  - Bigger responsibility on the user side

ORTC



Source: http://draft.ortc.org/

Go for Deep/Detailed API or ~~Go home~~!

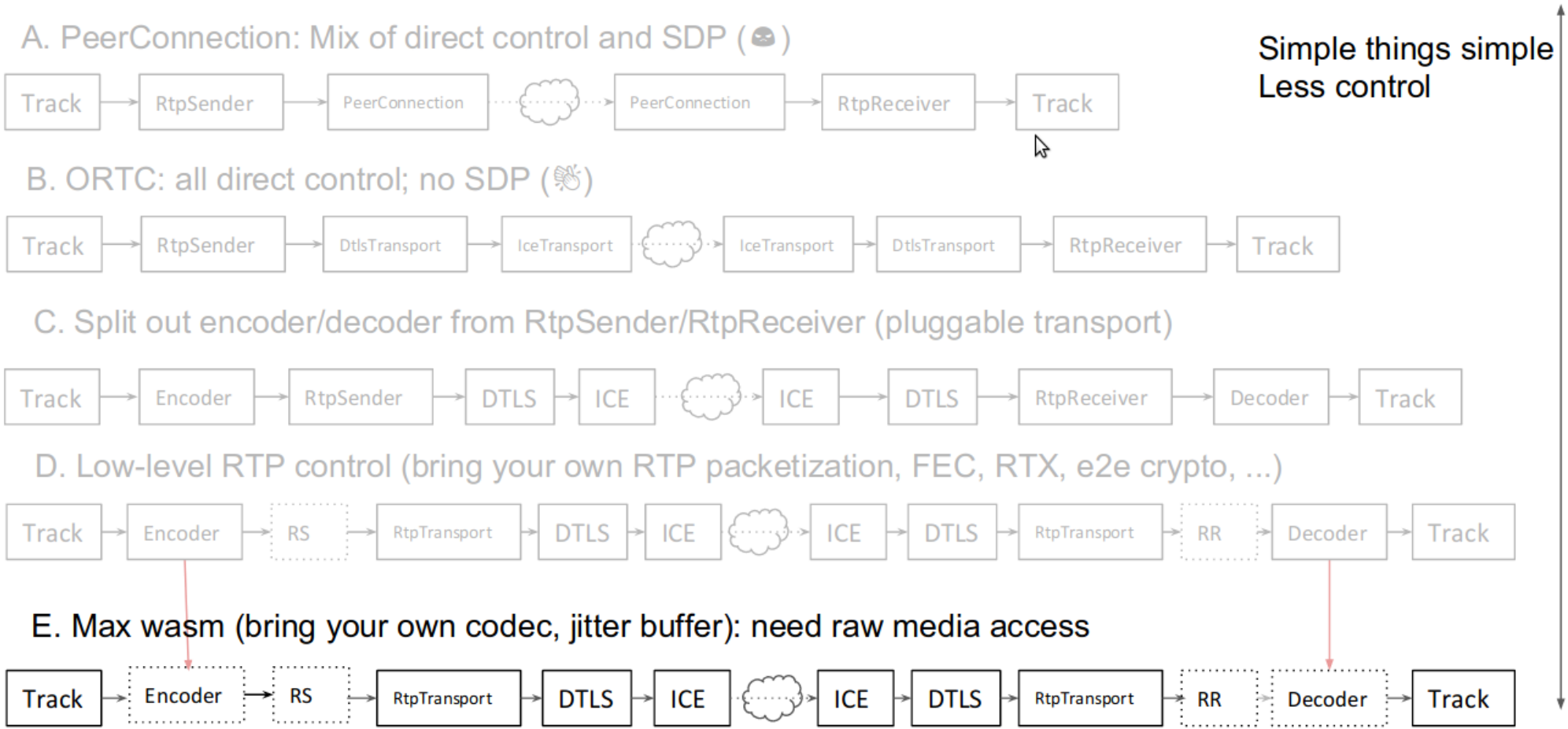
Lower level API

- Developers are demanding for more control
  - Deeper API requested
  - even deeper than ORTC
  - hand in hand with more responsibility
  - Vendors could differentiate themselves with implementation.
    - We could go back in time again to the closed source incompatibility hell? :-(
  - More control in developers hand, and more complexity!
    - A web developer usually is not a telecommunication expert
    - The first idea was that WebRTC 1.0 should hide complexity from developers, and give only moderate control on the multimedia session establishment.
      - Fast learning curve, avoid frustrated developers

With Great Power ..

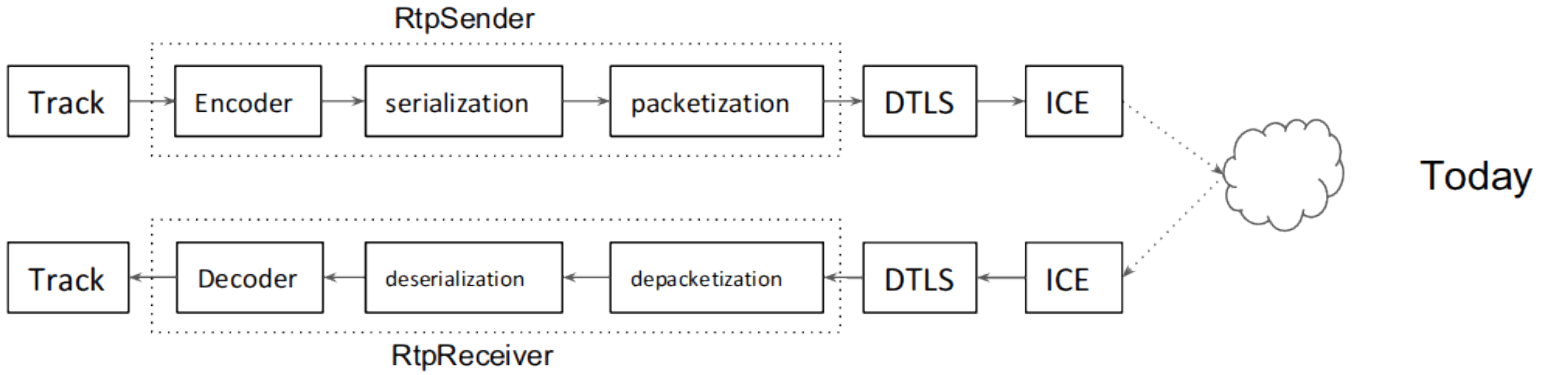
Source: https://flic.kr/p/TEEaFq

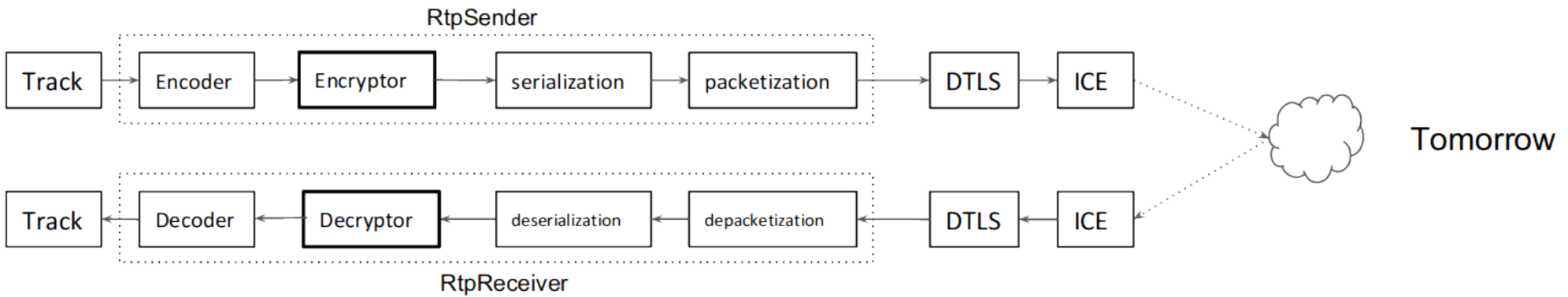
How deep is not too deep?



Source: https://www.w3.org/2011/04/webrtc/wiki/images/5/5c/WebRTCWG-2018-06-19.pdf

More detailed API

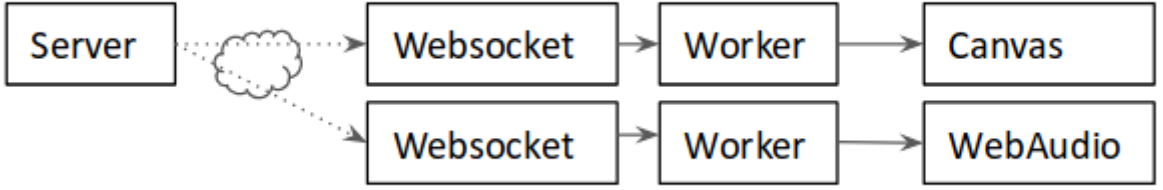


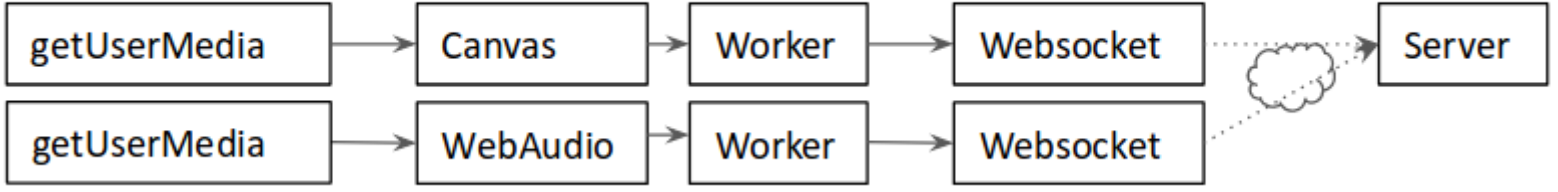


Source: https://lists.w3.org/Archives/Public/www-archive/2018Nov/att-0002/WebRTCWG-2018-10-23.pdf

WASM

- WebRTC hacks article:
  - https://webrtchacks.com/zoom-avoids-using-webrtc/
- WASM = Web Assembly
- Zoom
  - video/audio
  - encode/decode





ICE

ICE

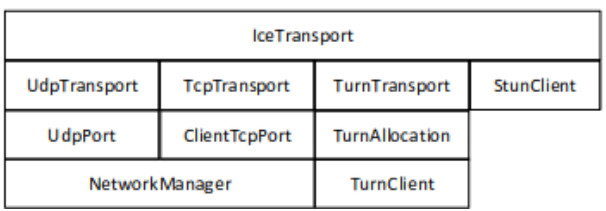
A. PeerConnection: Not standalone, uses SDP (😠)

B. WebRTC-ICE extension spec: standalone, no SDP (🐞)

C. ORTC: split gatherer/transport (supports forking)

D. FlexICE

E. SLICE



Simple things simple
Less control

More control
More complex

Source: https://www.w3.org/2011/04/webrtc/wiki/images/5/5c/WebRTCWG-2018-06-19.pdf

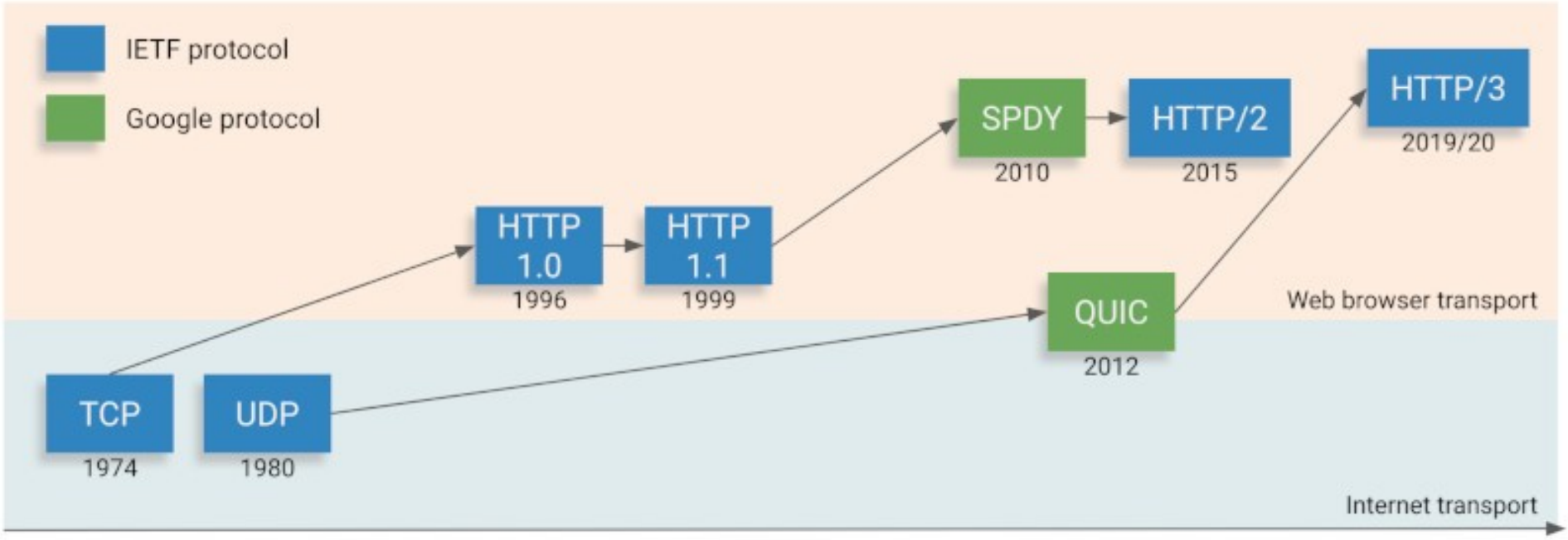
Pros/Cons

- WebRTC-ICE
  - allows for constructing an ICE agent separate from a PeerConnection, without SDP, suitable for use with other transports (QuicTransport).
- ORTC
  - also allows parallel forking. But it also requires more objects to be managed by the app (IceGatherer)
- FlexICE
  - also allows for control over ICE checking frequency/pausing, local candidate lifetimes, continual gathering, and timeouts for disconnect. But it requires the app to do more to get the advanced uses (you just get normal behaviour otherwise). New controls can be added incrementally.
- SLICE
  - allows the app to implement a custom ICE stack with the lowest-level primitives possible. But it requires the app use a library, because no one will be implementing their own ICE stack. Apps that don't need advance things can just use a high-level IceTransport. Those that do are capable of tweaking everything

QUIC

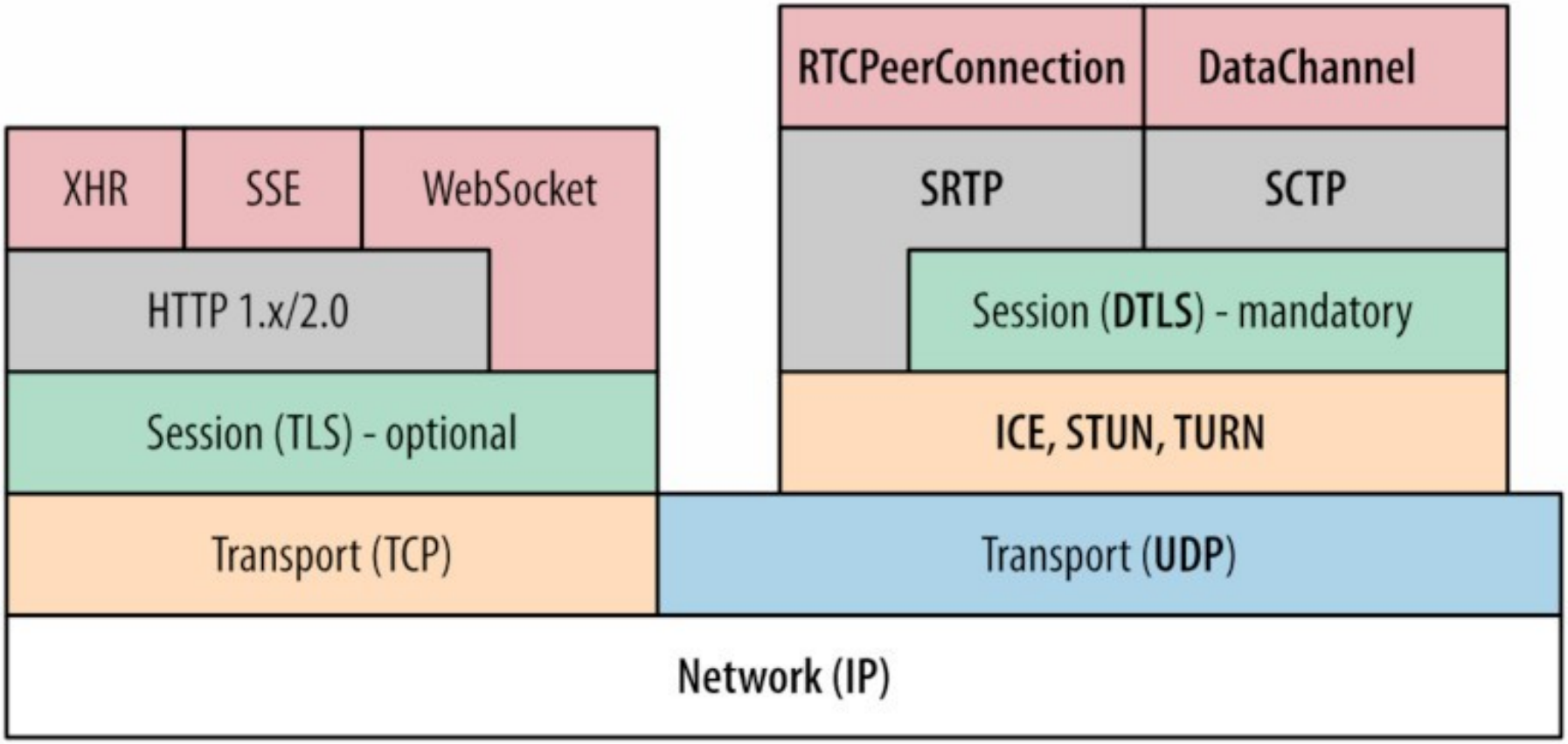
- A QUIC developed as HTTP/3 transport protocol
  - Currently only supports reliable transport
  - Built-in encryption, and congestion control
- DataChannel
  - SCTP => QUIC
- Bring Your Own (BYO) Transport. Replacement of RTP/RTCP?
  - RTP designed in the 1990-s. Maybe it’s time to redesign it?
  - QUIC-R transport (Colin Perkins, Jörg Ott)
    - R as realtime extension
    - Replacement of both MPEG-DASH(TCP) and RTP/RTCP(UDP)
    - Converged streaming and videoconferencing

Transport Protocol History



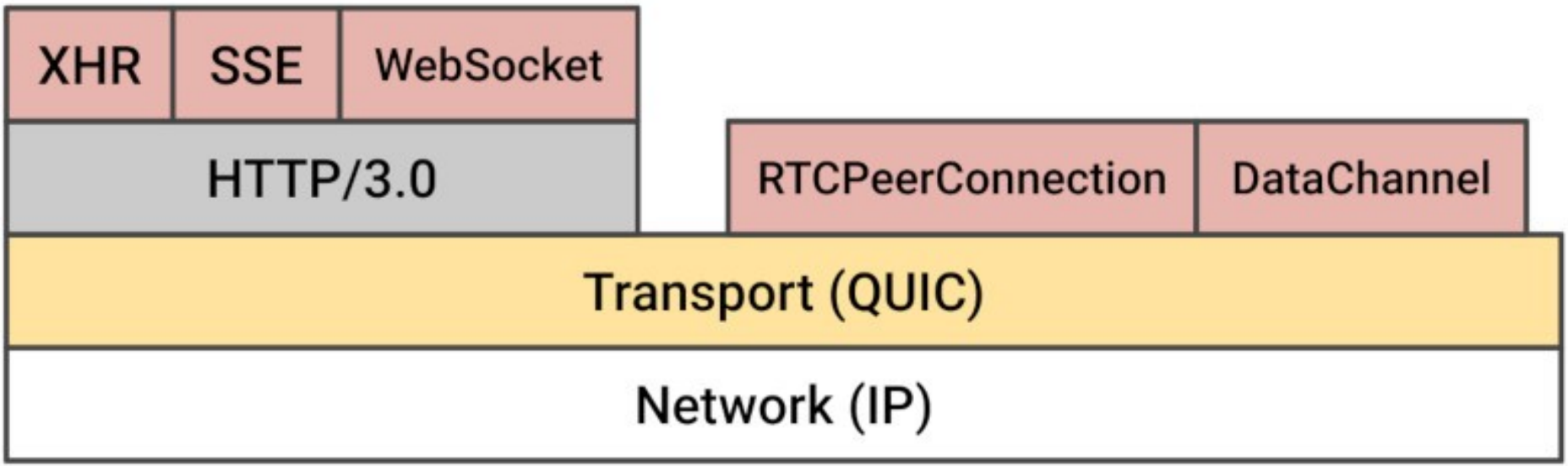
Source: https://bloggeek.me/who-needs-quic-in-webrtc/

WebRTC 1.0



Source: https://bloggeek.me/who-needs-quic-in-webrtc/

WebRTC-NV over QUIC

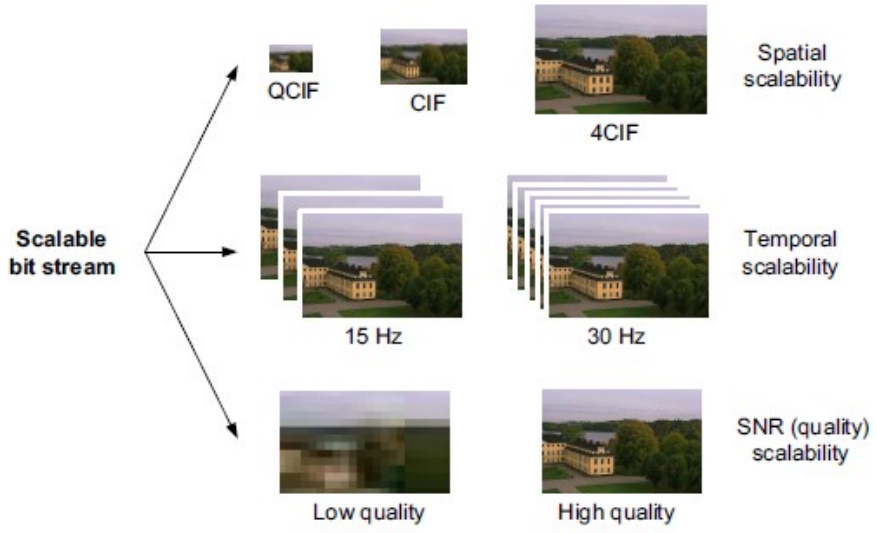


Source: https://bloggeek.me/who-needs-quic-in-webrtc/

AV1, SVC

- AV1 is in the pipe
  - Better quality
  - Less bandwidth
  - Optimised for high resolution (4k, 8k)
  - Little bit more CPU
- Scalable Video Coding SVC
  - Spatial
  - Temporal
  - Quality

Alliance for Open Media



KIFÜ

Docker

Containers are coming!

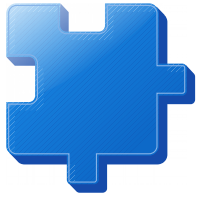
KIFÜ

Moving into a container

KIFÜ

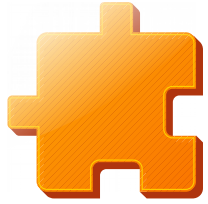
coTURN

coTURN



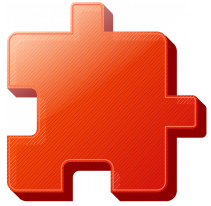
- Involved in development
  - Merged many PRs and handled issues
  - Security Fix
    - 2 CVE coordinated with Cisco
    - Still many open issues :(
  - Debian packaging
    - Thanks to Ferenc Wágner support
- Docker
  - Host networking (Docker bug)
    - NAT could also work with some limitations
  - Docker-compose for different backends
    - MongoDB, MySQL, Postgres, Redis, SQLite

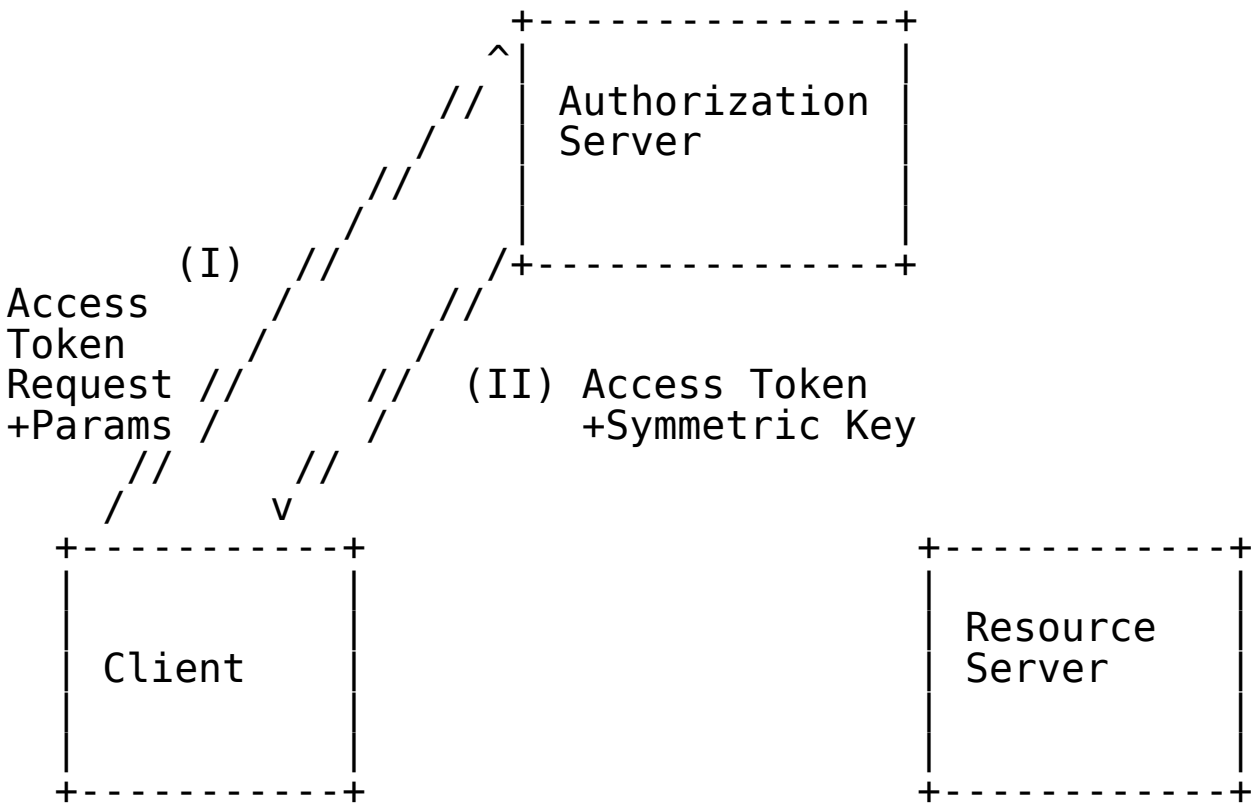
TURN OAuth credential



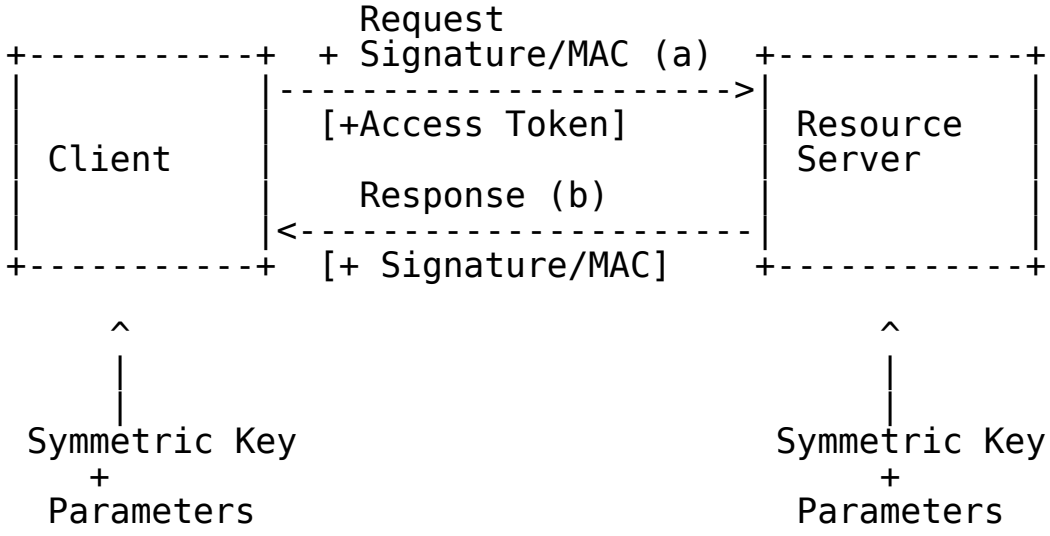
- Scoped credential
  - Time limited
  - Server limited
- Multiple Auth Server
  - co-located TURN
- It is an IETF Standard
  - Compared to other auth methods
    - REST is a discontinued draft
    - Classic LTC is not suitable for Web
      - JS app can’t keep credential in secret.

TURN OAuth PoP

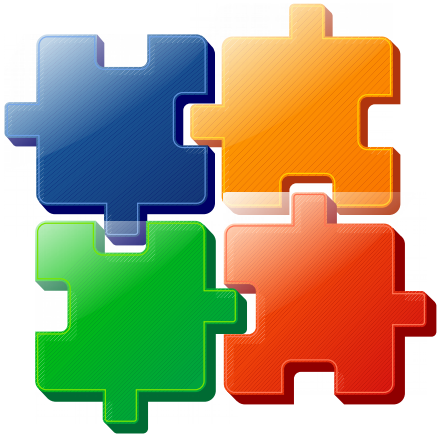




TURN OAuth PoP

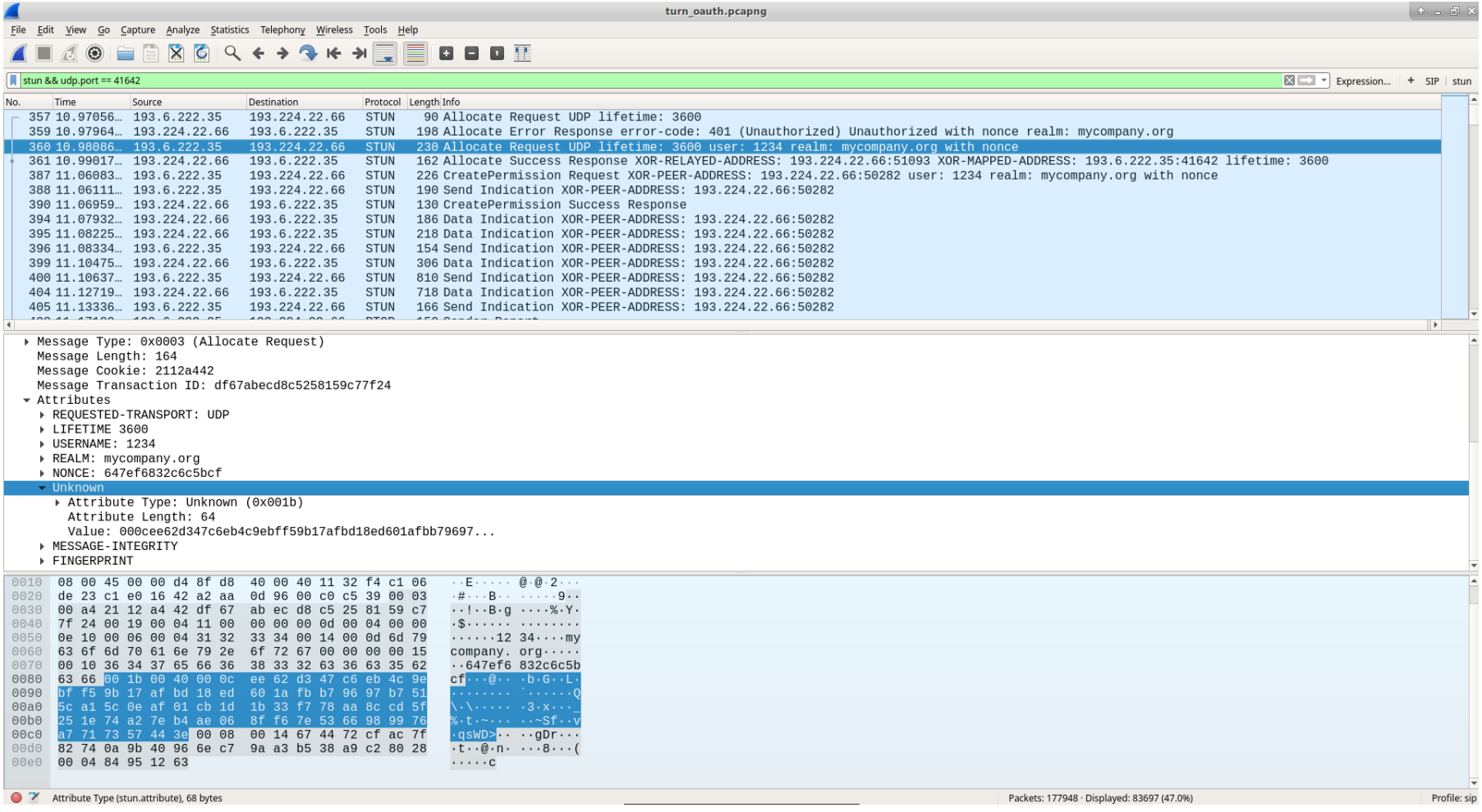


Firefox: WebRTC TURN OAuth



- OAuth Proof of Possession key distribution
- coTURN issue SHA1 length different for
  - Long Term Credential SHA1(MD5())
    - MD5 output 16 byte
  - OAuth SHA1 default input 20byte
- https://bugzilla.mozilla.org/show_bug.cgi?id=1247616
  - I am working implementation in Firefox TURN + OAUTH.
    - I have successfully authenticated against a coTURN server
  - We need in second phase to update token and credential periodically
    - iceRestart

“We believe in rough consensus and running code.”



KIFÜ

Advancing MultiPartyMeeting

MultipartyMeeting in Docker

- Open Source
  - https://github.com/misi/mm
- https://hub.docker.com/r/misi/mm/
- MultipartyMeeting Listens Multiple ports
  - Web Server (express), Signaling(socket.io),
    Selective Forwarding Unit (MediaSoup)
- Docker large port range NAT issue
  - https://success.docker.com/article/docker-compose-and-docker-run-hang-when-binding-a-large-port-range
  - Host networking (workaround)

Enhance Multiparty-Meeting Auth (OIDC)

- Enhance AAI integration
  - replace passport-dataporten to more generic
- Open ID Connect (OIDC)
- openid-client
  - https://www.npmjs.com/package/openid-client
  - passport
- Claim
  - Name, Picture
- SAML Satosa SAML <=> OIDC gateway
  - https://satosa.aai.niif.hu/.well-known/openid-configuration

KIFÜ

MultiPartyMeeting

Easy to use, easy to deploy

MultipartyMeeting Ansible Demo

- Easy Ansible based Setup
  - Requirements
    - Debian VM
    - a DNS name
    - modify config files
  - The script request Let’s Encrpyt certificate, and configures, docker, run image customize logo, etc.
- Demo setup in 10 min!
- https://github.com/misi/mm-ansible

Try MultipartyMeeting!

KIFÜ

E-learning integration

MM in Moodle module

UP2U

- Loose integration
  - https://github.com/misi/multipartymeeting-moodle
- Good feedback from pilot schools..
- Knockplop

Summary

- Follow the Standardization (IETF, W3C)
- Containers are coming (Docker, K8S)
  - RTC in container is not a low hanging fruit
- GÉANT: **STUN/TURN infrastructure pilot**
  - Try it: https://turn.geant.org
  - OAuth is in the pipe
- Try MultipartyMeeting, it is free, open, extendable!
  - OIDC, E-learning integration, etc.
- Goal: Serve the community communication needs with advanced reliable, extendable open source tools!

Summary – Next Steps

- Standardization
  - how to contribute to the standardisation?
- Containers are coming (Docker, K8S)
  - Are there better and easier to be integrated than containers?
- GÉANT: STUN/TURN infrastructure pilot
  - how to deploy and maintain at GÉANT level?
- OAuth / OIDC is in the pipe
  - GÉANT T&I /EduGAIN confederation supportive enough for OIDC?
- MultipartyMeeting
  - What is needed for a better service?

KIFÜ

Many thanks for Your attention!

Questions?