

A satellite-style world map showing continents in green and brown and oceans in blue. The text is overlaid in the center.

# Enable VoLTE/VoNR in IMS using WebRTC



Răzvan Crainea  
- 30th of April 2024 -



- Introduction
- IP Multimedia Subsystem
- Architecture
- eP-CSCF
- Conclusions
- “IMS” Working Group



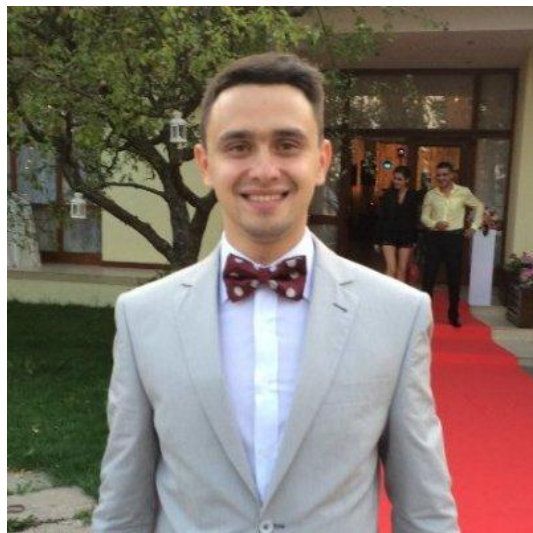
# Introduction

# About me

---



- Bucharest, Romania
- Working on the OpenSIPS since 2010
- OpenSIPS Core Developer
- SIPhub CTO
- Father of a 3yo



- Open-Source SIP Proxy/Server
- Flexible
  - 100+ modules
  - Programmable
- Highly Scalable
  - 20k calls per second
  - Millions simultaneous calls
- Handles SIP signalling
  - No media



- Session Border Controller
- Front-End to your VoIP Core
- Trunking
- Residential
- Load Balancer
- Call Center Queuing
- Virtual PBX



# OpenSIPS - The Open SIP Server



- high-performance, open source SIP server
- full RFC 3261 compliance
- used by carriers, telcos and ITSPs
- multi-functional
- multi-purpose
- programmable
- written in C
- modular



# Powering ITSPs and Telcos



AG Projects

be ip

crexendo  
Cloud Managed Telephony™

ippi

open IP

Téléphonie - Internet - Sécurité - Cloud

sureVoIP®

Budget  
Phone  
company

ecosmob  
bringing innovative technologies

KurpfalzTEL

MODULIS

snom

XConnect  
Interconnecting Our Digital World™

GULFSIP  
KEEP IN TOUCH

localphone  
Call global, pay local

CONNEX  
CONNECTING BUSINESS

RATETEL

VoiceTel

onsip

SIP<sub>2</sub>SIP

APPLIVE  
SIP Platform

Telappliant

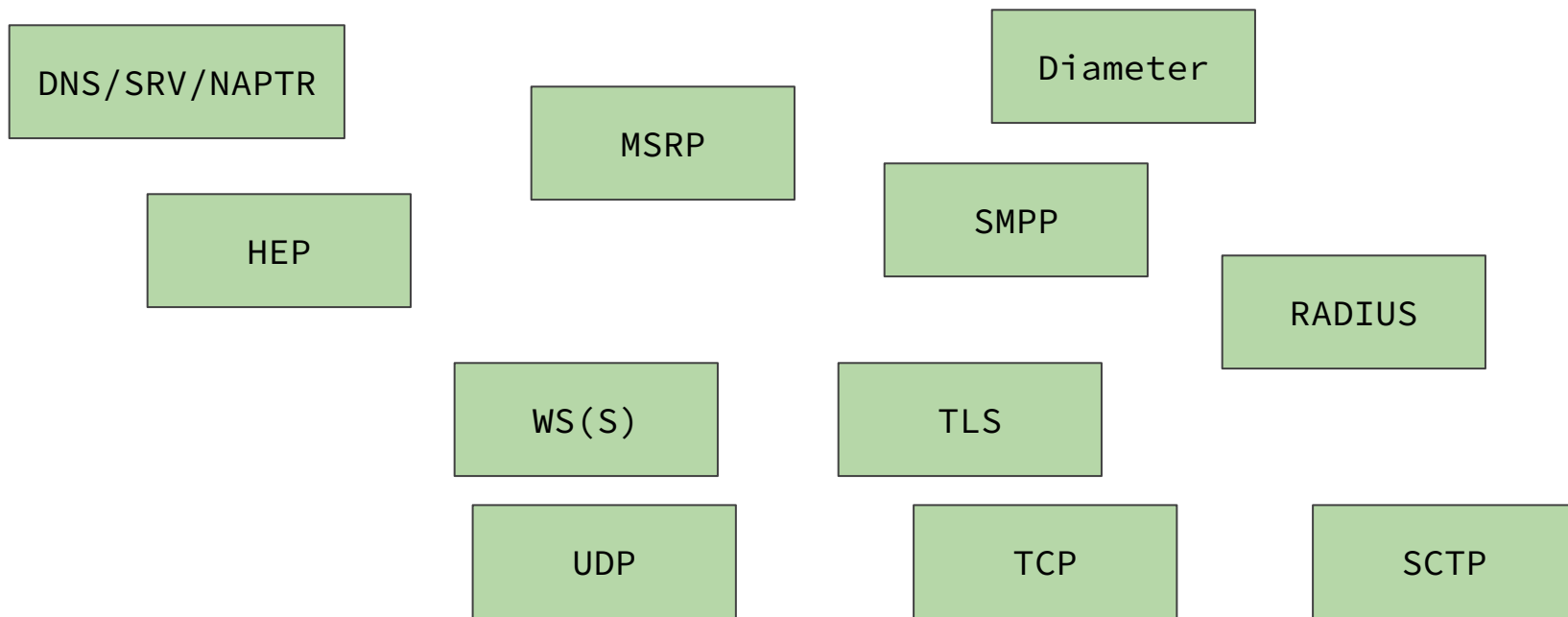
VoIPGRID

sourceVOX

VollI  
TALK IS CHEAP™



# OpenSIPS - Transport & App Protocols



RFC 8599  
SIP PN

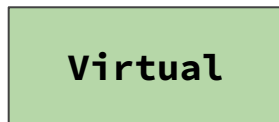
RFC 8760  
Digest Auth

SIP  
Presence

SIP  
B2BUA

RFC 8866  
SDP

# OpenSIPS Interfacing: SQL

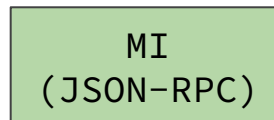


# OpenSIPS Interfacing: NoSQL



# OpenSIPS Interfacing: Others

---



- bespoke *scripting* language
- event-driven control of SIP
  - requests vs. replies
  - manipulate headers/body
- variables w/ scopes
  - process-private
  - SIP tx
  - SIP dialog
  - global

```
$acc_leg(onnet) = "0";

if (is_method("INVITE")) {
    do_accounting("db", "cdr|failed");

    # any non-ACK dialog should end quickly
    $DLG_timeout = 10;

    # create the dialog
    if (!create_dialog("B")) {
        xlog("[${ci}] WARNING: failed to create dialog
        route(CHECK_SYNTAX_EXTRA);
        send_reply(500, "Internal Server Error");
        exit;
    }
    set_dlg_sharing_tag("HA_TAG");
```

- **179** modules!
  - <https://opensips.org/Documentation/Modules-3-5>
- SIP registrar
- SIP Presence
- LCR + failover
- Load Balancing + failover
- topology hiding
- RTP relay
  - RTPProxy / RTPEngine / MediaProxy
- NAT traversal

```
$acc_leg(onnet) = "0";

if (is_method("INVITE")) {
    do_accounting("db", "cdr|failed");

    # any non-ACK dialog should end quickly
    $DLG_timeout = 10;

    # create the dialog
    if (!create_dialog("B")) {
        xlog("[${ci}] WARNING: failed to create dialog
        route(CHECK_SYNTAX_EXTRA);
        send_reply(500, "Internal Server Error");
        exit;
    }
    set_dlg_sharing_tag("HA_TAG");
```

# Build Class 4 Services

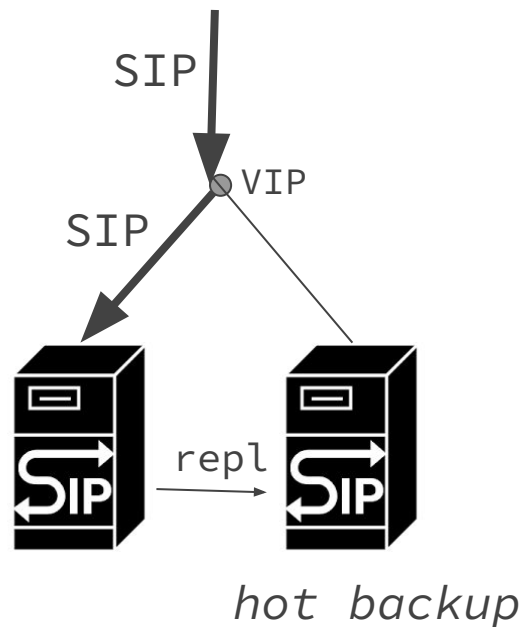


- Session Border Controller
- Wholesale Trunking
- SIP front-end (Registrations, Presence, etc.)
- SIP Redirect Services
  - LNP
  - LCR
  - CNAM
  - STIR/SHAKEN *signing*
  - STIR/SHAKEN *verification* ([stir shaken](#) module)



# Build Class 5 Services

- PBX
- Conferences\*
- Hunt Groups
- Call Pickup
- Call Parking
- IVRs\*
- Voicemail\*

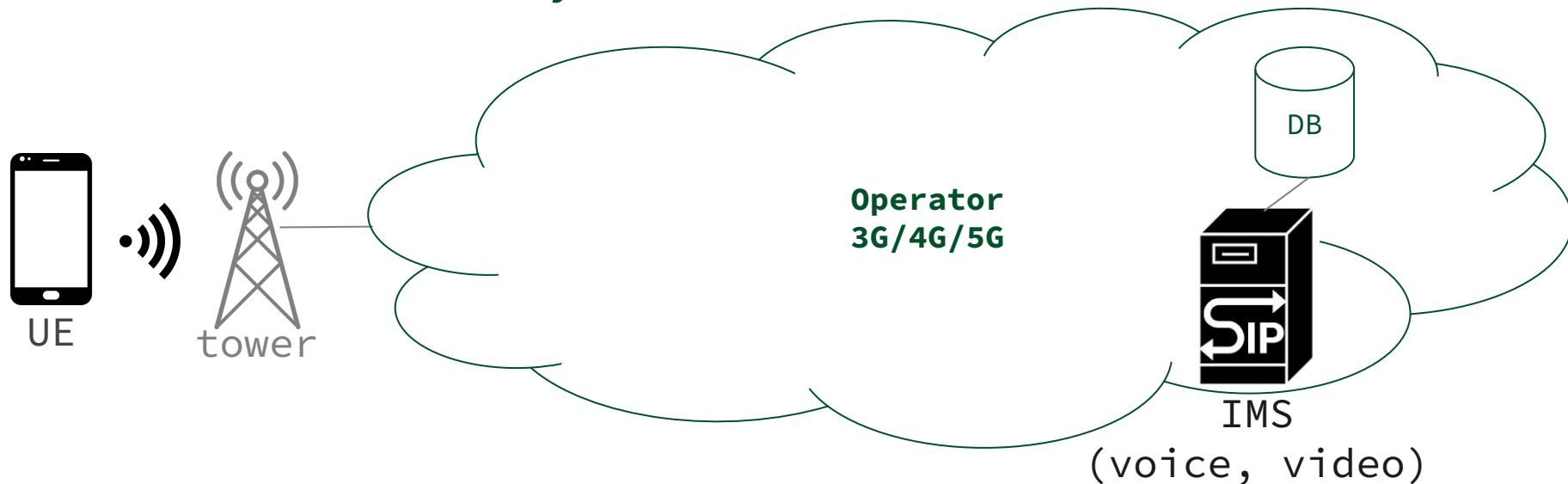


(\*) in tandem with a media server e.g. FreeSWITCH / Asterisk

IMS

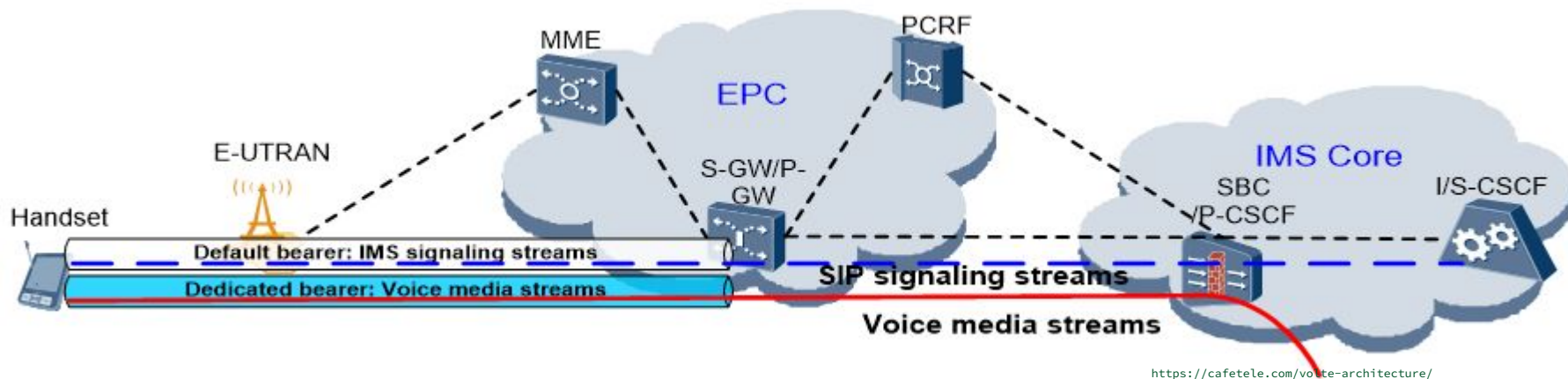
# IMS - simple terms

- **IP Multimedia Subsystem**



# IP Multimedia Subsystem

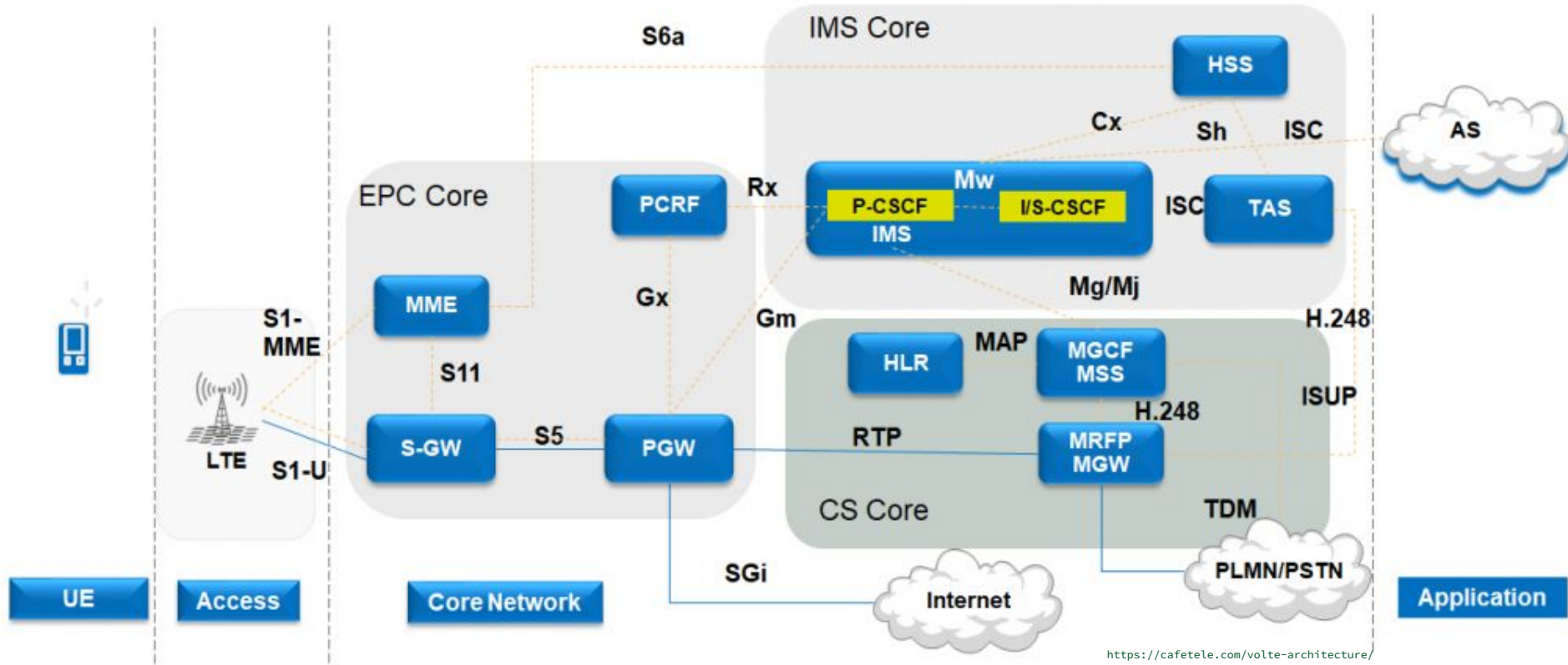
- architectural framework for delivering IP multimedia services
- describes interactions between all components
- modular design, open interfaces



- Voice over LTE (Long Term Evolution/4G)
  - One Voice Initiative, 2009, adopted by GSMA in 2010
  - GSMA PRD IR.92, IMS Profile for Voice and SMS
  - First release in 2012, 226 operators in 2020
- Improvements (over 3G/2G)
  - Fast call set-up
  - High Definition voice quality
  - Reduced background noise
  - Video calling

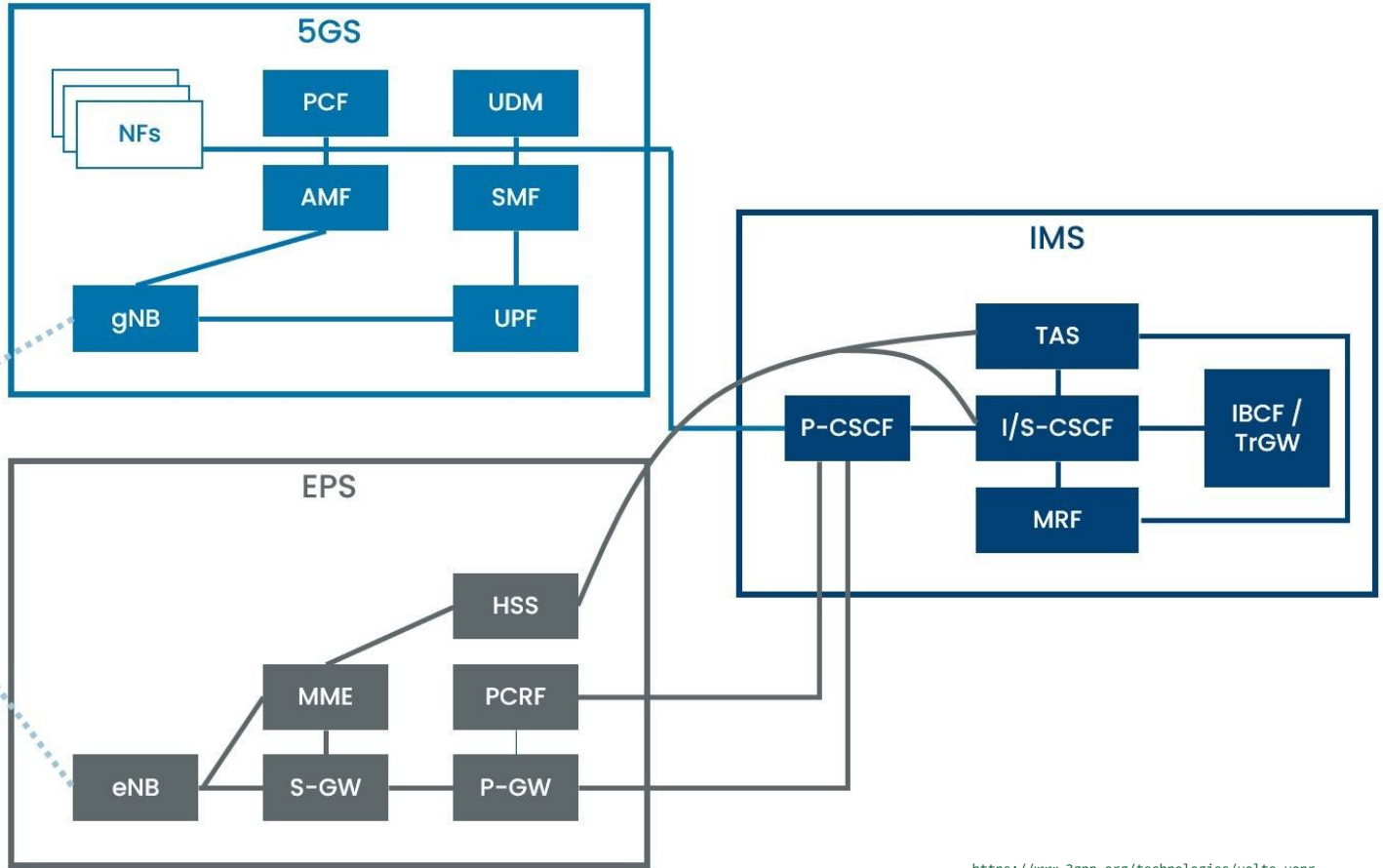


# VoLTE Network Architecture



- Voice over New Radio or Voice over 5G System
  - GSMA PRD NG.114, IMS Profile for Voice, Video and Messaging over 5GS
  - Specs released in August 2020
- Improvements (over VoLTE)
  - Better codecs support (AMR-WB)
  - Faster call set-up
  - Low latency capabilities
  - Allows fallback to VoLTE
  - Drops 2G and 3G



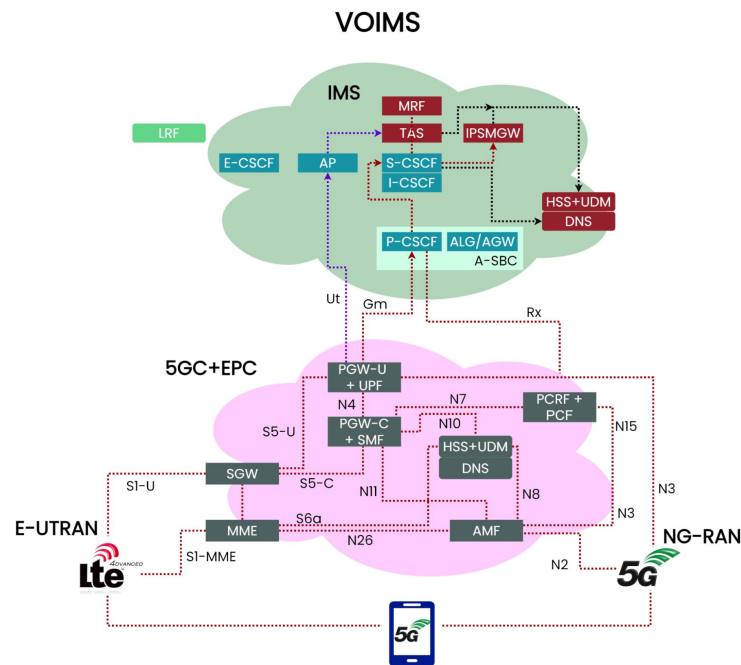


<https://www.3gpp.org/technologies/volte-vonr>



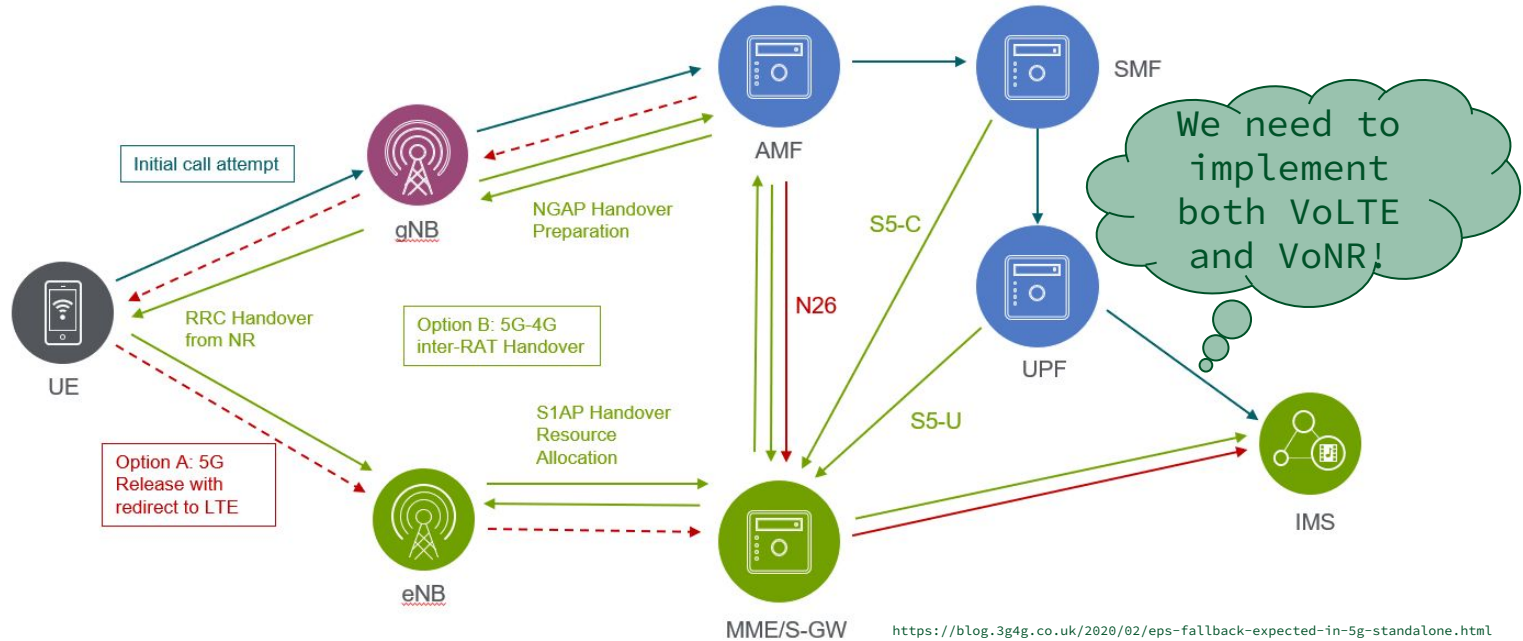
# VoNR vs VoLTE

- Different core architecture
- IMS architecture is the same
- Different interfaces
  - Diameter vs HTTP 2.0
- VoNR provides fallback
  - Switch call to VoLTE

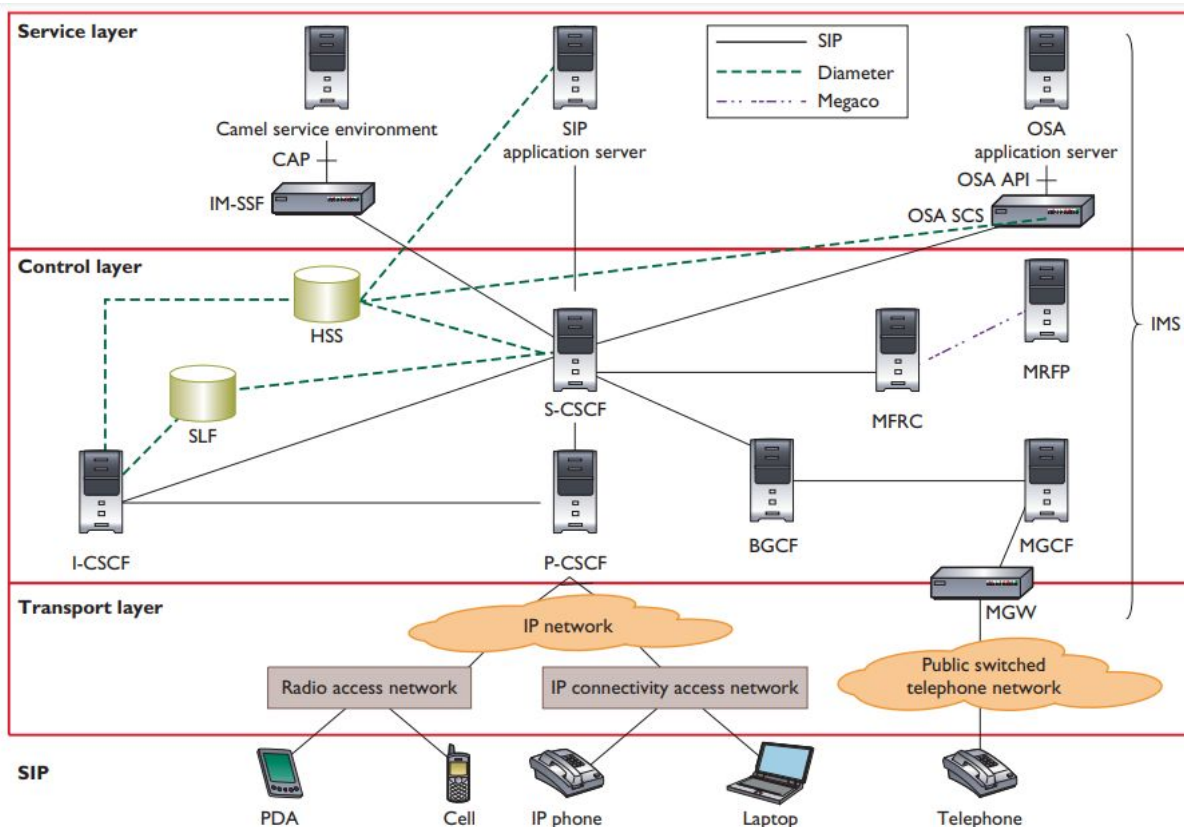


<https://telcomaglobal.com/p/vonr-call-flow>

# VoNR to VoLTE EPS fallback



# Architecture



SIP



PDA



Cell



IP phone



Laptop



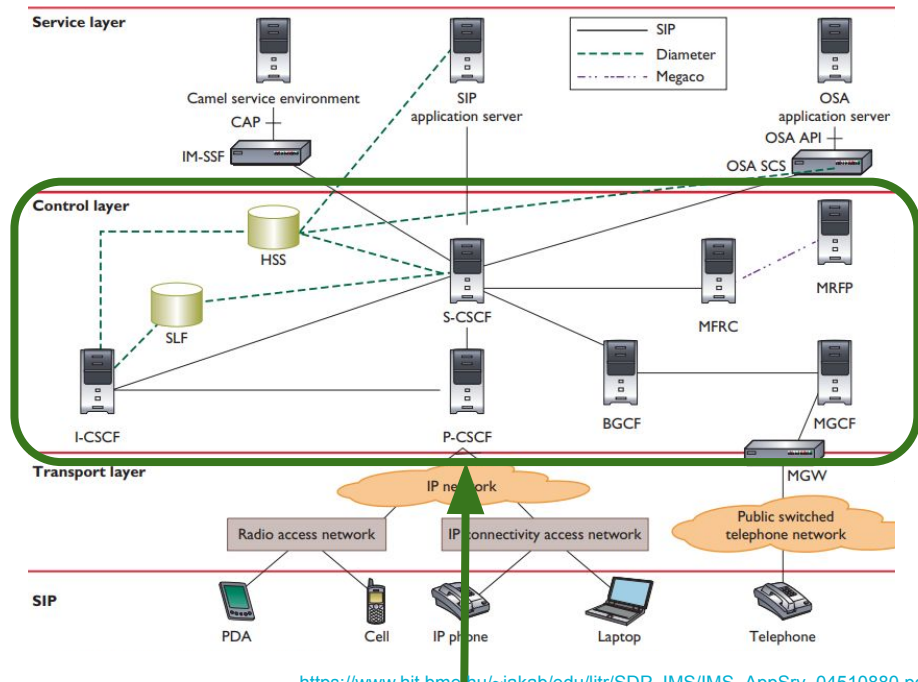
Telephone

BGCF: Breakout gateway control function  
 Camel: Customized applications for mobile networks using enhanced logic  
 CSCF: Call session control function  
 HSS: Home subscriber server  
 I-CSCF: Interrogating CSCF  
 IMS: IP multimedia subsystem  
 IM-SSF: IP multimedia service switching function  
 MFRC: Multimedia resource function control  
 MGCF: Media gateway control function

MGW: Media gateway  
 MRFP: Media resource function processor  
 OSA: Open services architecture  
 P-CSCF: Proxy CSCF  
 SCS: Service capability server  
 S-CSCF: Serving CSCF  
 SIP: Session Initiation Protocol  
 SLF: Subscriber location function

# Control Layer

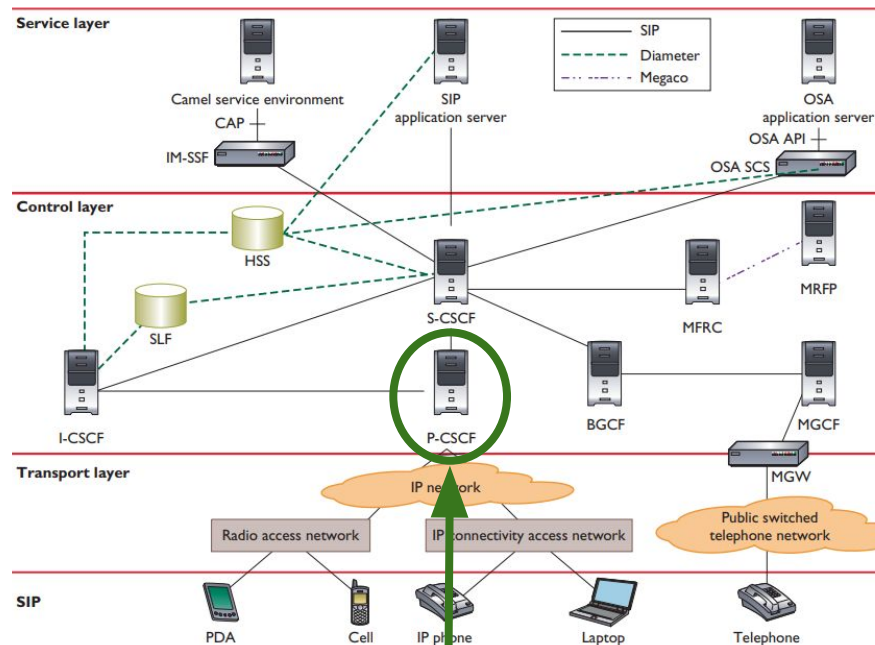
- the core of IMS
- NF == IETF protocols
  - SIP
  - Diameter
  - MSRP
  - SDP / RTP / RTCP
  - XCAP
  - NG: **HTTP/2**



[https://www.hit.bme.hu/~jakab/edu/ittr/SDP\\_IMS/IMS\\_AppSrv\\_04510880.pdf](https://www.hit.bme.hu/~jakab/edu/ittr/SDP_IMS/IMS_AppSrv_04510880.pdf)

# Proxy CSCF

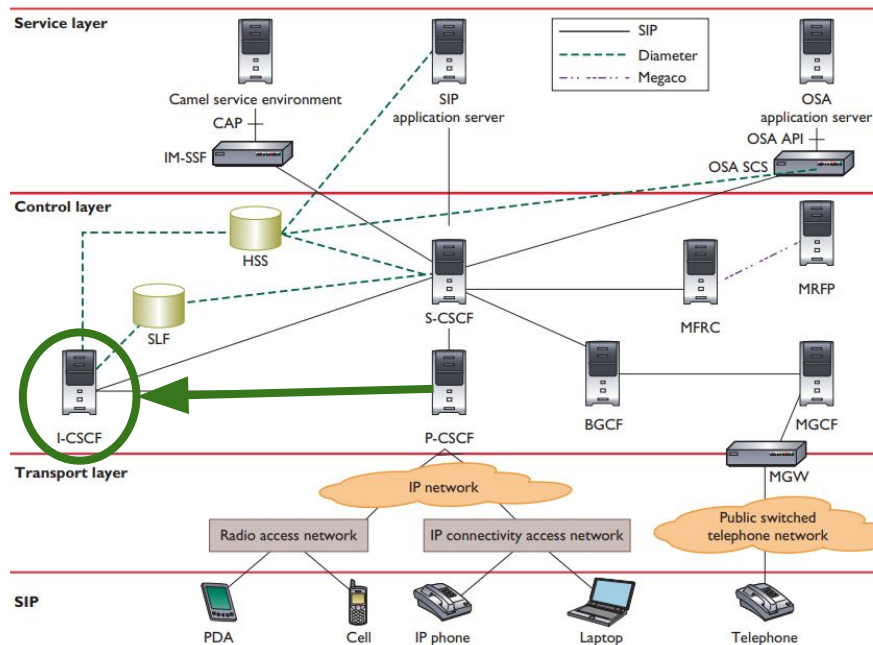
- a SIP proxy
- may offer SBC features
- first point of contact
- discovery by IMS terminals
  - DHCP
  - pre-configuration
- Enforces security with UE
  - replay/spoofing attacks
  - privacy
- generates charging records



[https://www.hit.bme.hu/~jakab/edu/litr/SDP\\_IMS/IMS\\_AppSrv\\_04510880.pdf](https://www.hit.bme.hu/~jakab/edu/litr/SDP_IMS/IMS_AppSrv_04510880.pdf)

# Interrogating CSCF

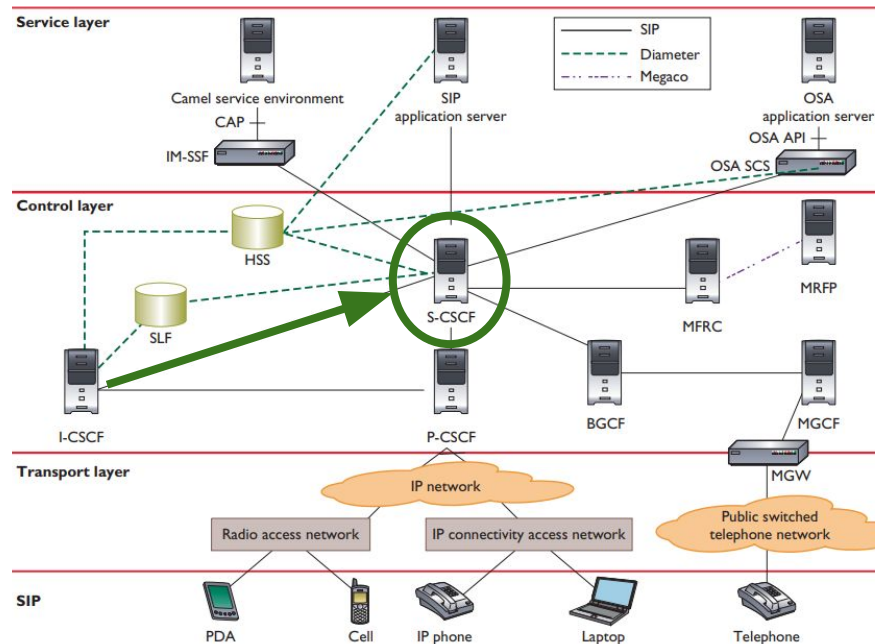
- a SIP proxy
- edge of administrative domain
- published in the DNS server
- entrypoint for all SIP transactions



[https://www.hit.bme.hu/~jakab/edu/litr/SDP\\_IMS/IMS\\_AppSrv\\_04510880.pdf](https://www.hit.bme.hu/~jakab/edu/litr/SDP_IMS/IMS_AppSrv_04510880.pdf)

# Serving CSCF

- central node
- registers users
- provides services
- routes SIP requests
- billing information
- SST
- interrogates HSS
  - authentication & authorization
  - user profiles

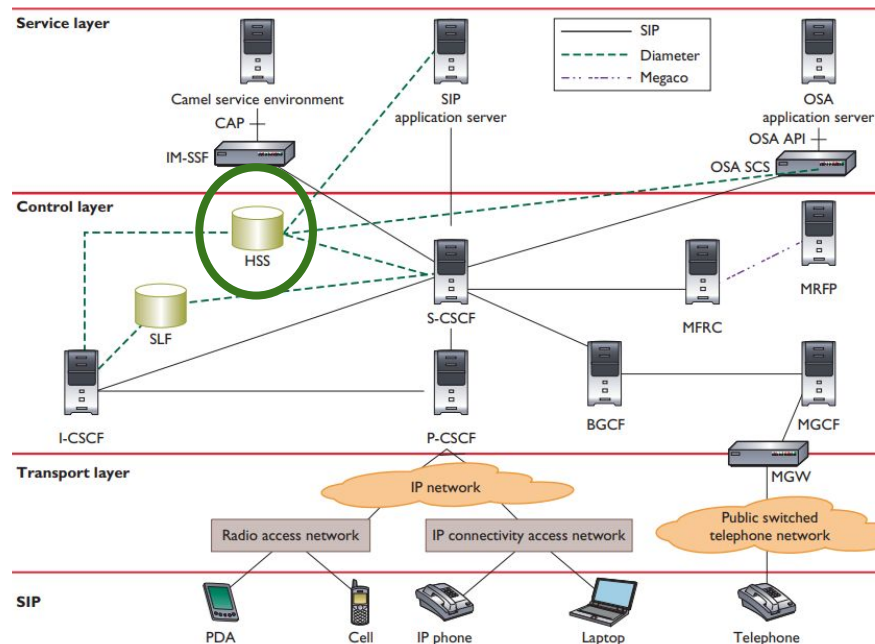


[https://www.hit.bme.hu/~jakab/edu/litr/SDP\\_IMS/IMS\\_AppSrv\\_04510880.pdf](https://www.hit.bme.hu/~jakab/edu/litr/SDP_IMS/IMS_AppSrv_04510880.pdf)



# HSS - Home Subscriber Server

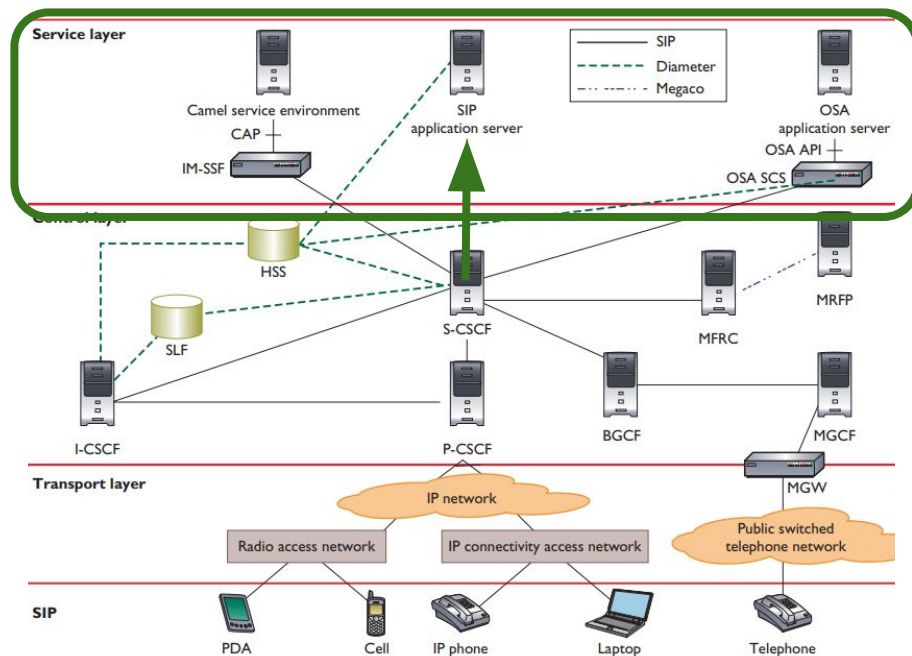
- master user DB
- supports NF which handle calls/sessions
- stores AA information
- provides info about users' locations
- implements Diameter



[https://www.hit.bme.hu/~jakab/edu/litr/SDP\\_IMS/IMS\\_AppSrv\\_04510880.pdf](https://www.hit.bme.hu/~jakab/edu/litr/SDP_IMS/IMS_AppSrv_04510880.pdf)

# Service Layer

- provides MM services
- an Application Server
  - hosts services
  - executes services
  - uses SIP protocol
    - redirect server
    - proxy server
    - origination UA
    - termination UA
    - B2B UA

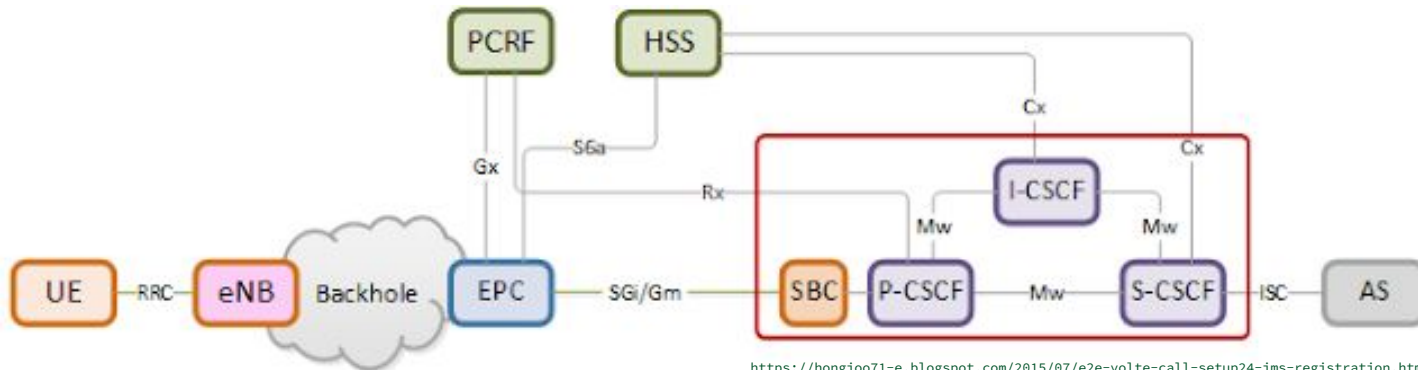


[https://www.hit.bme.hu/~jakab/edu/litr/SDP\\_IMS/IMS\\_AppSrv\\_04510880.pdf](https://www.hit.bme.hu/~jakab/edu/litr/SDP_IMS/IMS_AppSrv_04510880.pdf)

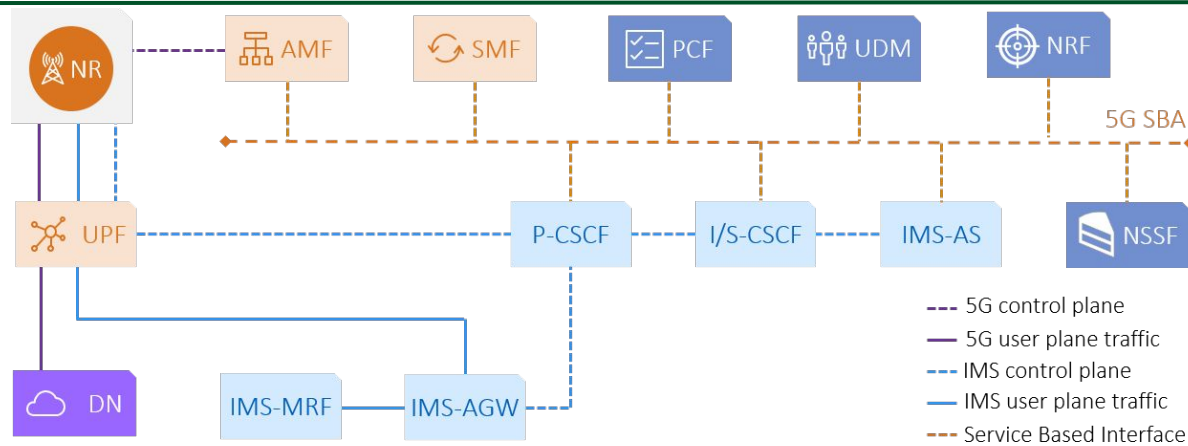
---

## Entry point of UE in IMS

- Provides a secure channel between UE and IMS
- RFC 3329 – Security Mechanism Agreement (SIP)
- Signaling
  - IPsec tunnels + AKAv1 authentication
  - TLS + AKAv2 authentication
- Media
  - SDES & DTLS-SRTP for RTP
  - TLS over MSRP
  - TLS & certificates for UDPTL/BFCP



- Proxy/Interrogating/Serving Call Session Control Function
  - SIP Signaling (Gm, Mw interface)
  - Diameter (Cx, Dx, Rx interfaces)
  - IMS AKA - mutual authentication between UE and IMS core (IPSec)



<https://hongjoo71-e.blogspot.com/2015/07/e2e-volte-call-setup24-ims-registration.html>

- Proxy/Interrogating/Serving Call Session Control Function
  - SIP Signaling (IMS control plane)
  - HTTP 2.0 implementation (for Service Based Interface)

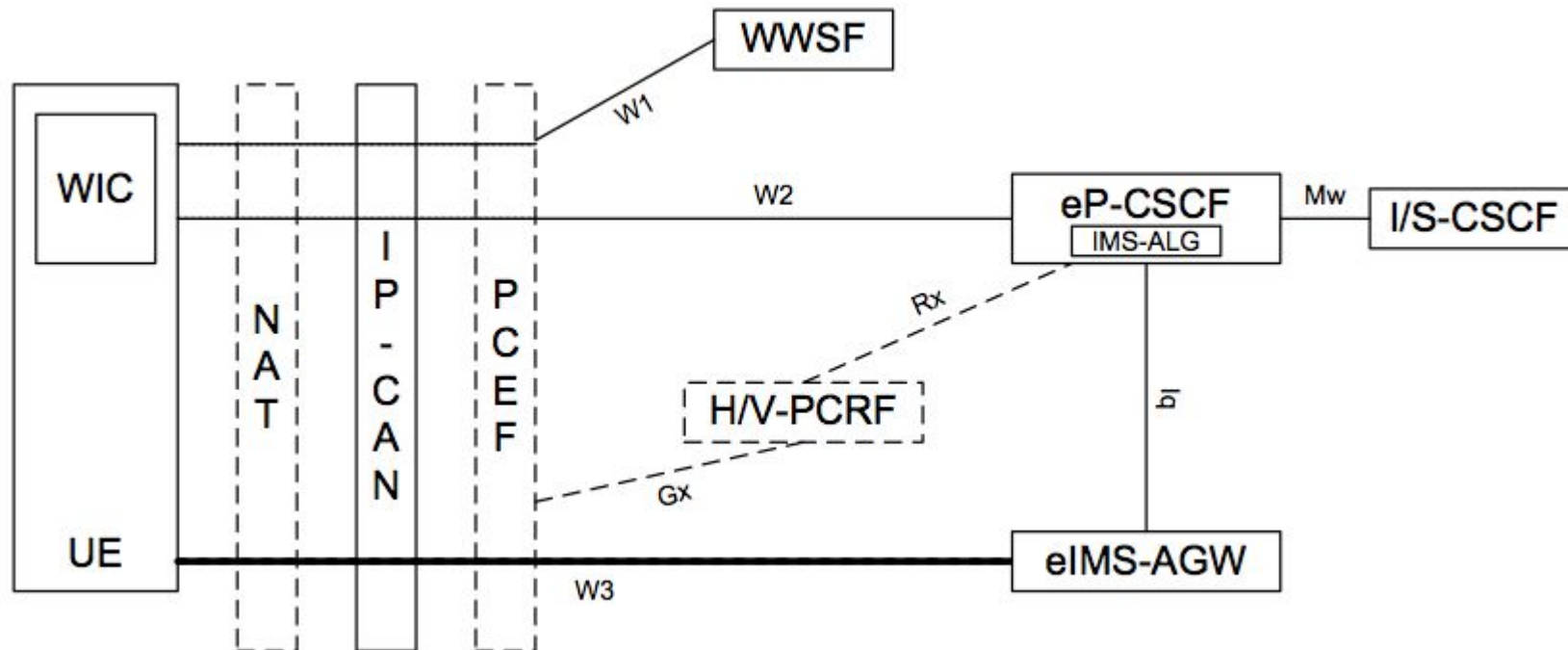
eP-CSCF

---

## P-CSCF enhanced for WebRTC

- Introduced in 3GPP TR 23.701 (2013–2014)
- Came along with the popularity of WebRTC
- Goal is to provide unified services
- How you can access IMS features from a browser
- Does not enforce a signaling protocol
  - SIP over WebSockets are preferred

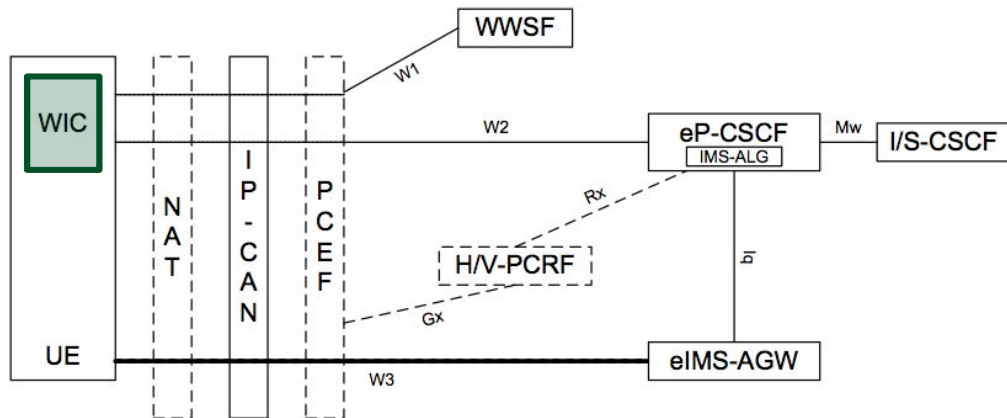
# eP-CSCF architecture





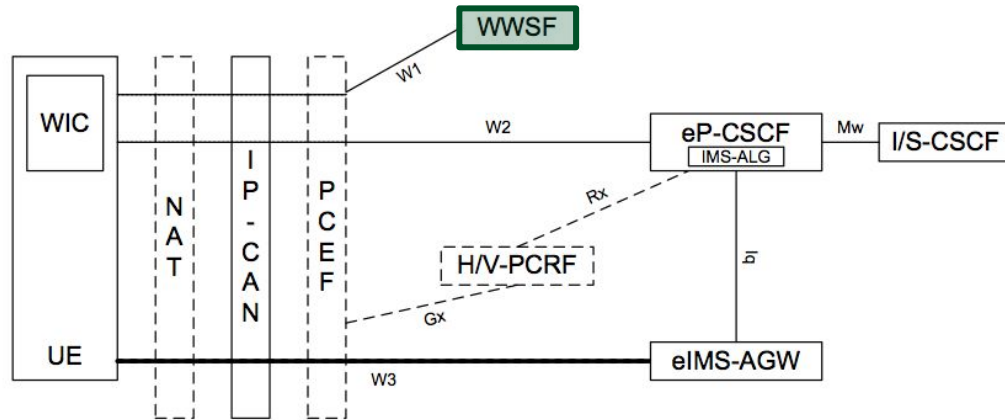
## WebRTC IMS Client

- WebRTC Javascript based application
- Downloaded from the WWSF
- Provides logic and APIs to access the IMS



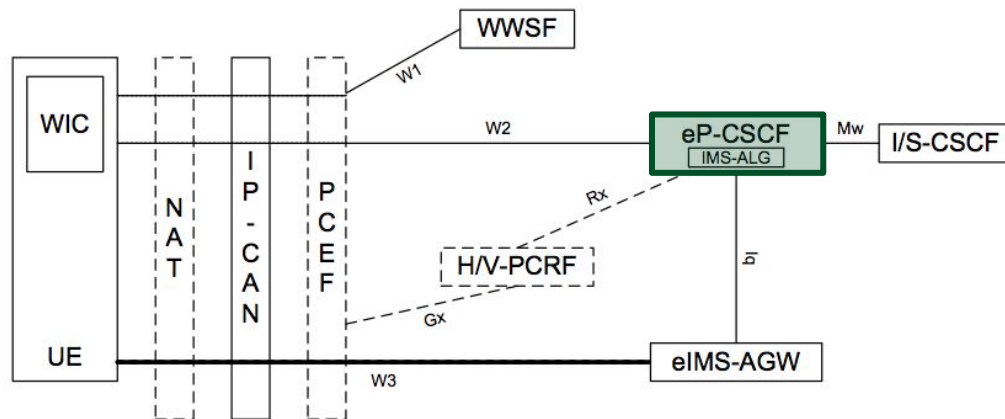
## WebRTC Web Server Function

- Web Server that hosts the WIC application
- Also referred as WebRTC Application Controller (WAC)
- Can handle authentication & authorization as well



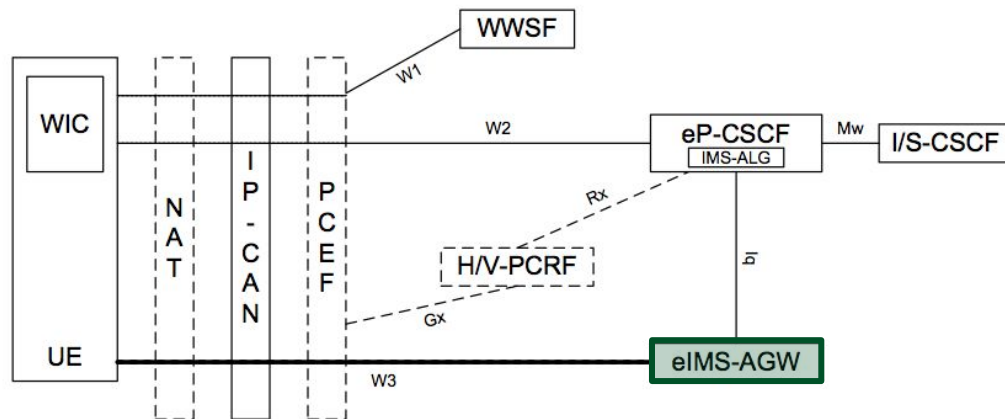
## P-CSCF enhanced for WebRTC

- Acts as a gateway from WebRTC to SIP
- Ensures a trusted channel between UE and IMS core
- “Normalizes” traffic towards IMS core

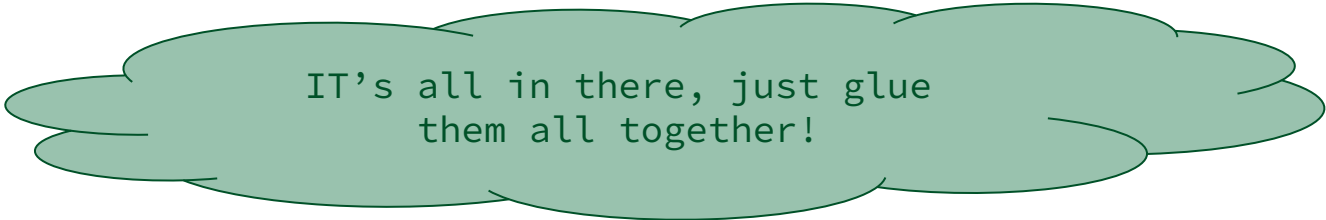


## IMS Access GateWay enhanced for WebRTC

- Handles media gatewaying
- Encryption/Decryption, Transcoding
- ICE, STUN, TURN



- Can already act as a (standard) P-CSCF
- Provides SIP over Secure WebSocket transport
- Provides AKA authentication
- Use rtpengine for media eIMS-AGW functionalities

A light green, hand-drawn cloud-like shape with a thin black outline, containing the text "IT's all in there, just glue them all together!".

IT's all in there, just glue  
them all together!

# Conclusions

- OpenSIPS is a versatile SIP Proxy/Server
- IMS enhances operator's networks with voice/video
- Use OpenSIPS as an IMS core
- eP-CSCF provides Web access to IMS

# OpenSIPS Working Groups



- OpenSIPS 3.5 release is IMS focused
- IMS is a complex topic
- exchange information/ideas between several parties
  - what are the industry needs?
  - which 3GPP specs are relevant?
  - what IETF protocols are required? In what scenarios?
- ... before considering any development!

# The “IMS” OWG



- gathers people with interest in IMS
- The more inputs, the better solution
- Goal: to draft, design and implement IMS support in OpenSIPS
- ML: <http://lists.opensips.org/cgi-bin/mailman/listinfo/wg-ims>
  - public discussions
  - free to join
- GHub Wiki: <https://github.com/OpenSIPS/opensips/wiki/IMS-OpenSIPS-Working-Group>

<https://summit.opensips.org>



# Take-Away Message

Use OpenSIPS 3.5 to build your own  
IMS VoLTE/VoNR infrastructure!

- Răzvan Crainea
  - @razvancrainea
  - razvan@opensips.org

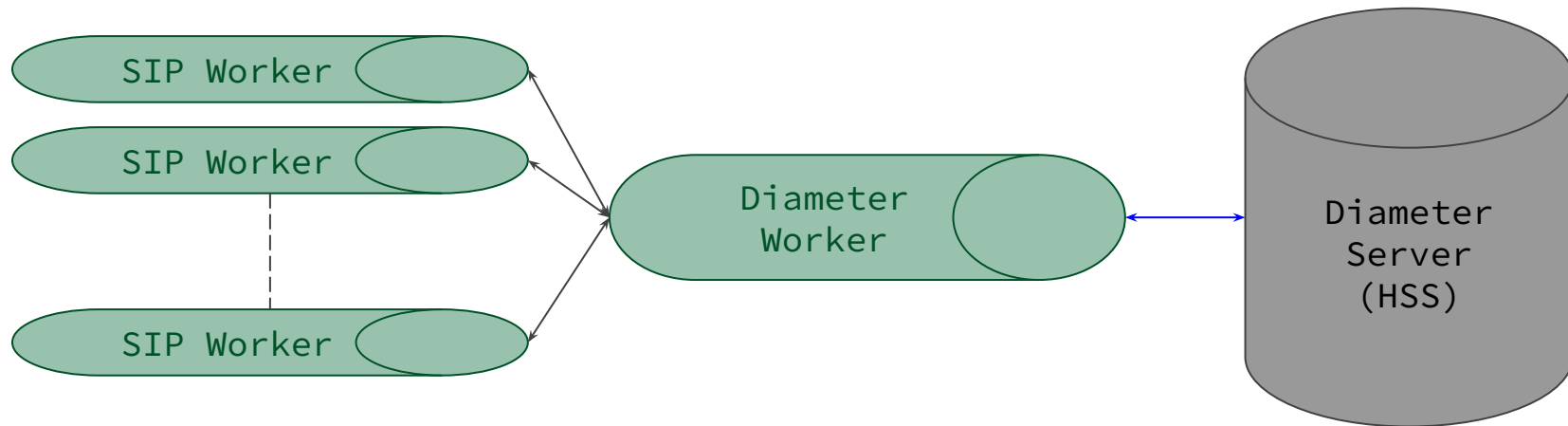
# OpenSIPS Implementation

- Provide a generic method of handling Diameter commands
  - Commands are “hand-crafted” in the script
    - Provides the ability to tune every single parameter
    - Fine grained inspection of the response
  - Provide samples with default behavior
- Commands can be handled both synchronous and asynchronous
- Act as a Diameter server
  - Handle commands from HSS (Push Profile, Registration Termination)
  - Access to the request/reply in script
  - Trigger additional actions

# Diameter Interface Implementation



- Built on top of **freeDiameter** Open Source project
- Multi-process (OpenSIPS) vs Single-process (Diameter)



# HTTP 2.0 Interface

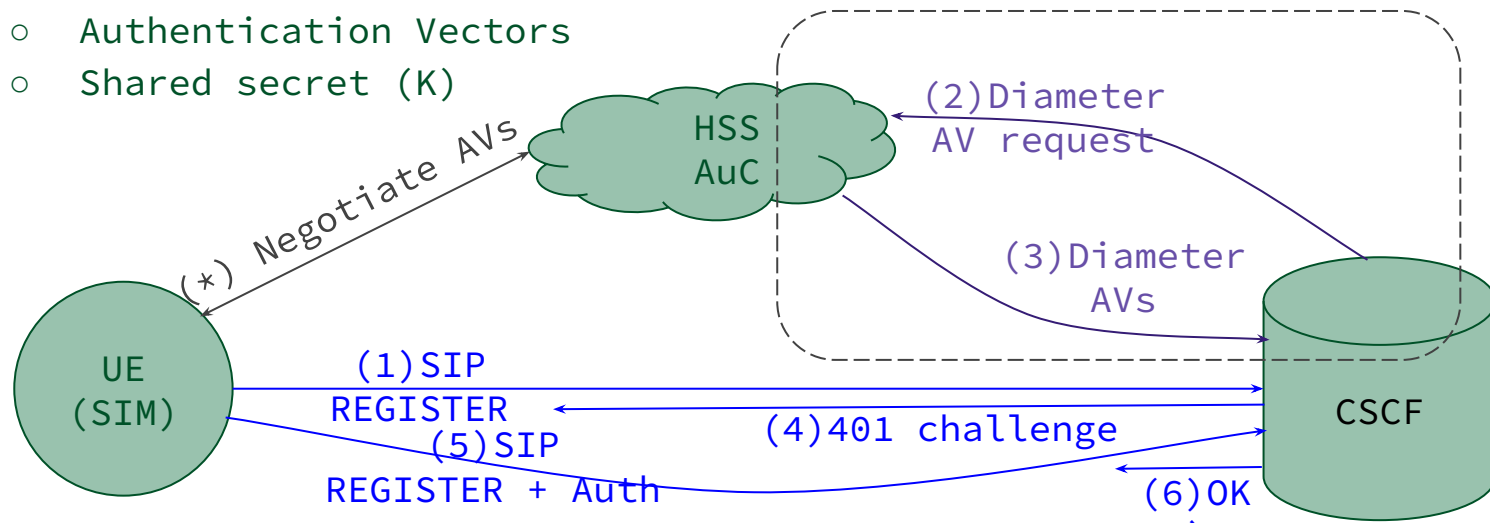
- Handling similar to Diameter
  - Commands are “hand-crafted” in the script
- Client side
  - `rest_client` module in OpenSIPS
  - `libcurl` - already supports HTTP 2.0
- Server side
  - `nghttp2` - implementation of HTTP 2.0 server
  - Dedicated process for handling requests
  - Dispatch requests to any available workers





- Authentication and Key Agreement

- Mutual authentication
- One time passwords
- Authentication Vectors
- Shared secret (K)



- RAND - Random number
  - AUT - Authentication token
  - XRES - Signed Result
  - CK - Cipher Key
  - IK - Integrity Key
- } Auth Challenge
- } Auth Response
- } Network Auth (IPSec)

- Auth\_aka module
  - Builds the necessary headers for challenges
  - Parses the response and authenticates the UA
  - Does **not** fetch the Authentication Vectors
  - Provides an interface to provide Authentication Vectors
- Authentication Vectors managers
  - “Transport” layer for fetching AVs
  - Modules
    - ✓ aka\_av\_diameter
    - ✓ aka\_av\_http2
    - ✓ aka\_av\_route

- AKA<sub>v1</sub> is susceptible to man-in-the-middle attacks
- Internet Protocol Security
  - Authentication and secure encrypted communication
- IMS AKA AVs
  - Integrity key (IK) and Cipher key (CK)
  - Used by P-CSCF to create a tunnel with UE
- Implementation
  - Dynamically created tunnels
  - Can not use classic VPN servers (StrongSwan)
  - XFRM interface or libmnl library



- 
- Immune to man-in-the-middle attacks
  - AKA<sub>v1</sub>, but masks IK and CK
    - Use derived values IK' and CK'
  - ETSI TS 133 203 v12 (2015)
    - No longer need IPsec
    - Communication over TLS/WebRTC