Overview of 3GPP SA WG6

SA6 Leadership:

Suresh Chitturi (Samsung Research)	3GPP SA WG6 Chairman
Alan Soloway (Qualcomm Technologies)	3GPP SA WG6 Vice-Chair
Jukka Vialen (Airbus)	3GPP SA WG6 Vice-Chair

Contributors:

Basavaraj Pattan (Samsung)	Rapporteur: CAPIF, SEAL
Camilo Solano (Ericsson) `	Rapporteur: MCIOPS
Dave Chater-Lea (Motorola Solutions)	Rapporteur: MCSMI, MCLog
Dom Lazara (Motorola Solutions)	Rapporteur: MCPTT, MCLoc
Jerry Shih (AT&T)	Rapporteur: MCData
Kees Verweij (The Police of the Netherlands)	Rapporteur: MCover5GS
Martin Oettl (Nokia)	Rapporteur: FRMCS/MONASTERY
Niranth Amogh (Huawei)	Rapporteur: CFA, MCVideo, V2XAPP, UASAPP
Nishant Gupta (Samsung)	Rapporteur: EDGEAPP
Peter Monnes (Harris)	Rapporteur: MCCI
Shao WeiXiang (ZTE)	Rapporteur: FFAPP

Outline

- Introduction to SA6
  - History and Evolution of SA6
  - Rel-16 / Rel-17 Overviews
- Mission Critical Topics
- Vertical Industry Enablement
- Conclusions

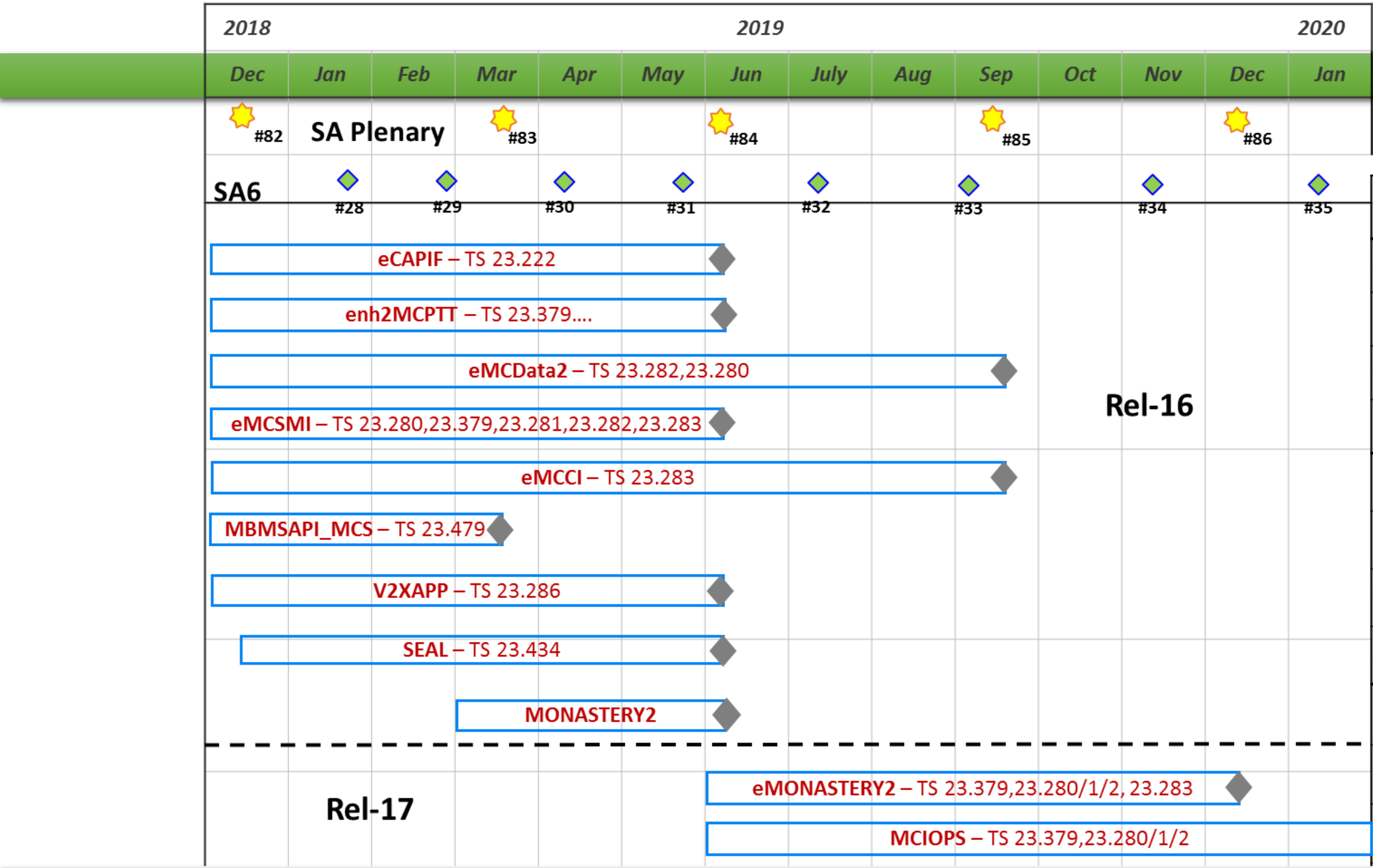
Outline

- Introduction to SA6
  - History and Evolution of SA6
  - Rel-16 / Rel-17 Overviews
- Mission Critical Topics
- Vertical Industry Enablement
- Conclusions

History and Evolution – SA6

- 3GPP identified as the home for global Mission Critical Services (MCX) Standards
  - Over 600 user requirements with inputs from TETRA, P25 and mobile broadband industry
  - New Working Group dedicated for Mission Critical Applications (SA6) – first expansion in 20 years!
- First global MCPTT standard published in 2016 (Rel-13)
  - MC standardization continues to evolve….
- SA6 expands its Terms of Reference (ToR) in June 2017
  - Critical Communications and related verticals (e.g. railways)
  - Other applications to support industry verticals
  - Northbound and device Application Programming Interfaces (APIs) for the above applications
  - Common API framework to support 3GPP northbound API development efforts

SA6 Work-Items



2018 2019 2020

Dec Jan Feb Mar Apr May Jun July Aug Sep Oct Nov Dec Jan

SA Plenary #82 #83 #84 #85 #86

SA6 #28 #29 #30 #31 #32 #33 #34 #35

eCAPIF – TS 23.222

enh2MCPTT – TS 23.379….

eMCData2 – TS 23.282,23.280

eMCSMI – TS 23.280,23.379,23.281,23.282,23.283

eMCCI – TS 23.283

MBMSAPI_MCS – TS 23.479

V2XAPP – TS 23.286

SEAL – TS 23.434

MONASTERY2

Rel-16

Rel-17

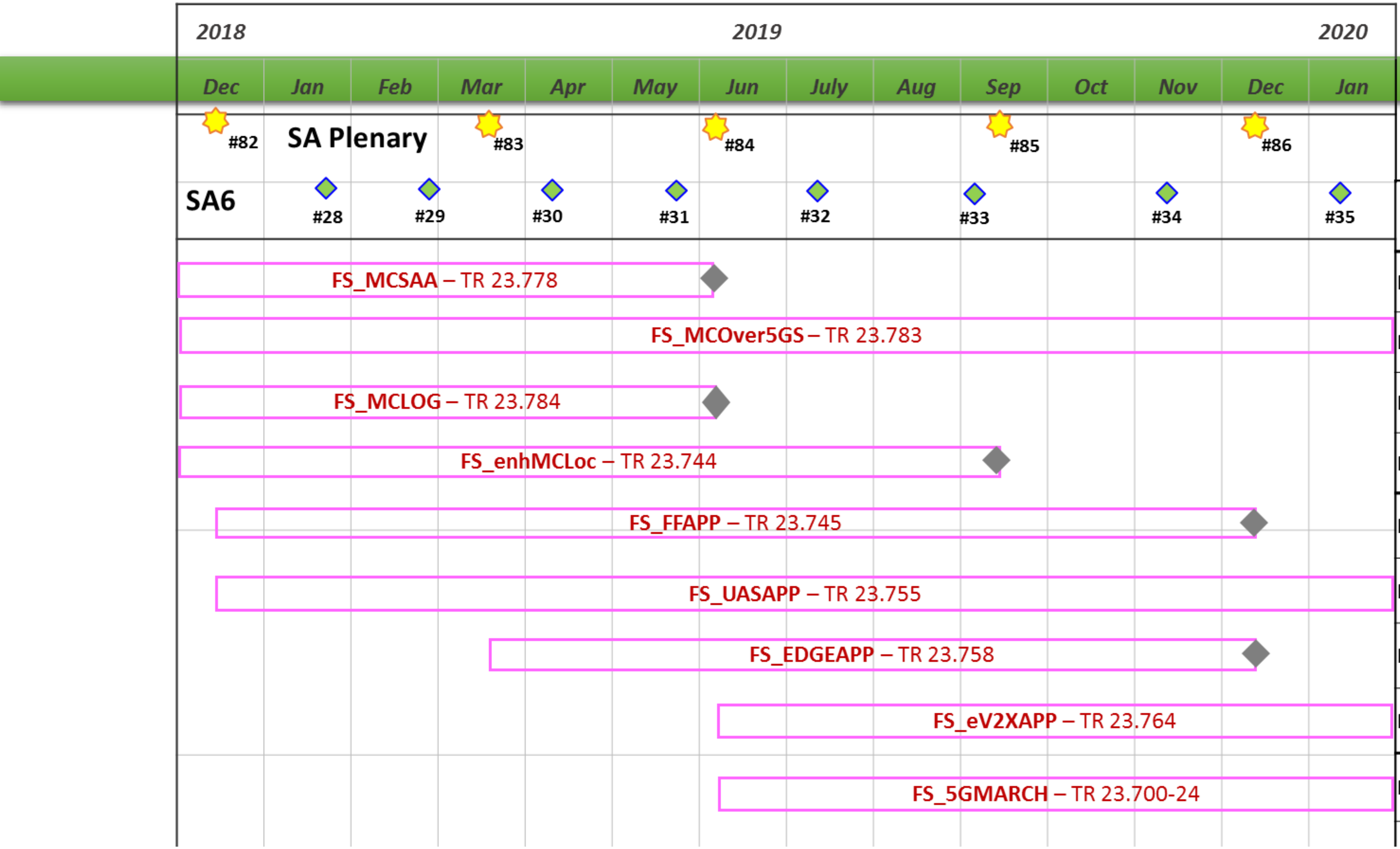
eMONASTERY2 – TS 23.379,23.280/1/2, 23.283

MCIOPS – TS 23.379,23.280/1/2

Work-Items

Completion Status (before SA6#32)	
eCAPIF	100%
enh2MCPTT	100%
eMCData2	90%
eMCSMI	100%
eMCCI	70%
MBMSAPI_MCS	100%
V2XAPP	95%
SEAL	95%
MONASTERY2	100%
eMONASTERY2	0%
MCIOPS	0%

SA6 Studies



2018 | 2019 | 2020

Dec | Jan | Feb | Mar | Apr | May | Jun | July | Aug | Sep | Oct | Nov | Dec | Jan

SA Plenary: #82, #83, #84, #85, #86

SA6: #28, #29, #30, #31, #32, #33, #34, #35

FS_MCSAA – TR 23.778

FS_MCOver5GS – TR 23.783

FS_MCLOG – TR 23.784

FS_enhMCLoc – TR 23.744

FS_FFAPP – TR 23.745

FS_UASAPP – TR 23.755

FS_EDGEAPP – TR 23.758

FS_eV2XAPP – TR 23.764

FS_5GMARCH – TR 23.700-24

Study-Items

Completion Status (before SA6#32)

FS_MCSAA	100%
FS_MCOver5GS	40%
FS_MCLOG	100%
FS_enhMCLoc	60%
FS_FFAPP	15%
FS_UASAPP	10%
FS_EDGEAPP	35%
FS_eV2XAPP	0%
FS_5GMARCH	0%

Outline

- Introduction to SA6
  - History and Evolution of SA6
  - Rel-16 / Rel-17 Overviews
- Mission Critical Topics
- Vertical Industry Enablement
- Conclusions

Mission Critical Common Functional Architecture (CFA)

Purpose and Scope

- A common functional architecture to support all MC services (i.e., MCPTT, MCVideo, MCData) including the common application plane and signalling plane entities.
- Purpose is to re-use the common functionalities across different MC services.

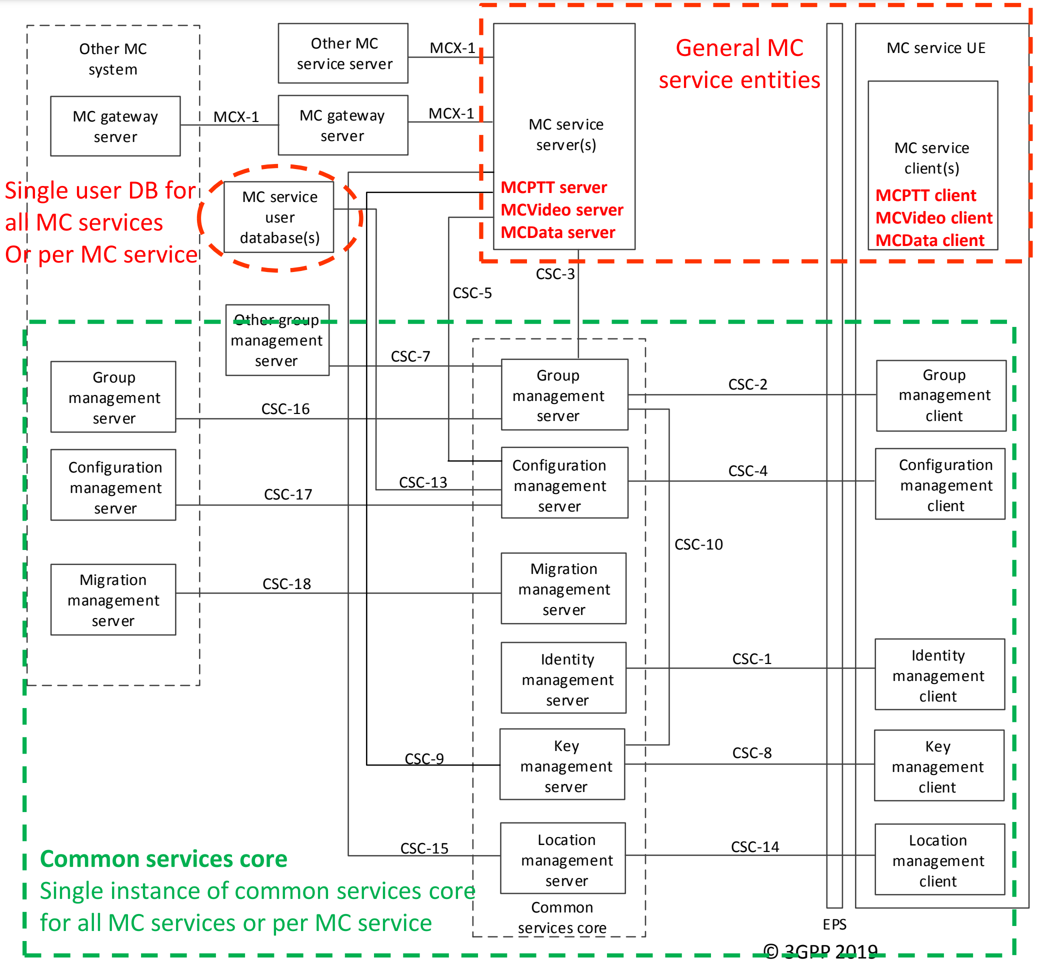
Key features

- CFA to support mission critical services can be used for public safety applications and also for general commercial applications e.g. utility companies and railways.
- Common services core functions (e.g. group management, configuration management, identity management, key management, location management)
- Supports on-network (Uu based unicast and multicast) and off-network (PC5) operations

CFA – Architecture

Key Functional Entities

- Application Plane client and servers
  - Group mgmt: Groups information mgmt (CRUDN)
  - Configuration mgmt: UE, service info configurations
  - Identity mgmt: Supports authentication
  - Key mgmt: Supports security aspects (encryption)
  - Location mgmt: Mgmt of user location information
  - Migration mgmt: Migration of users between systems
  - Functional alias mgmt: Support railways functional alias
- Signalling Plane
  - SIP entities: Compliant with external reference points of IMS. (User agent, SIP AS, SIP core, Diameter proxy)
  - HTTP entities: HTTP messaging support (HTTP client, HTTP proxy, HTTP server)



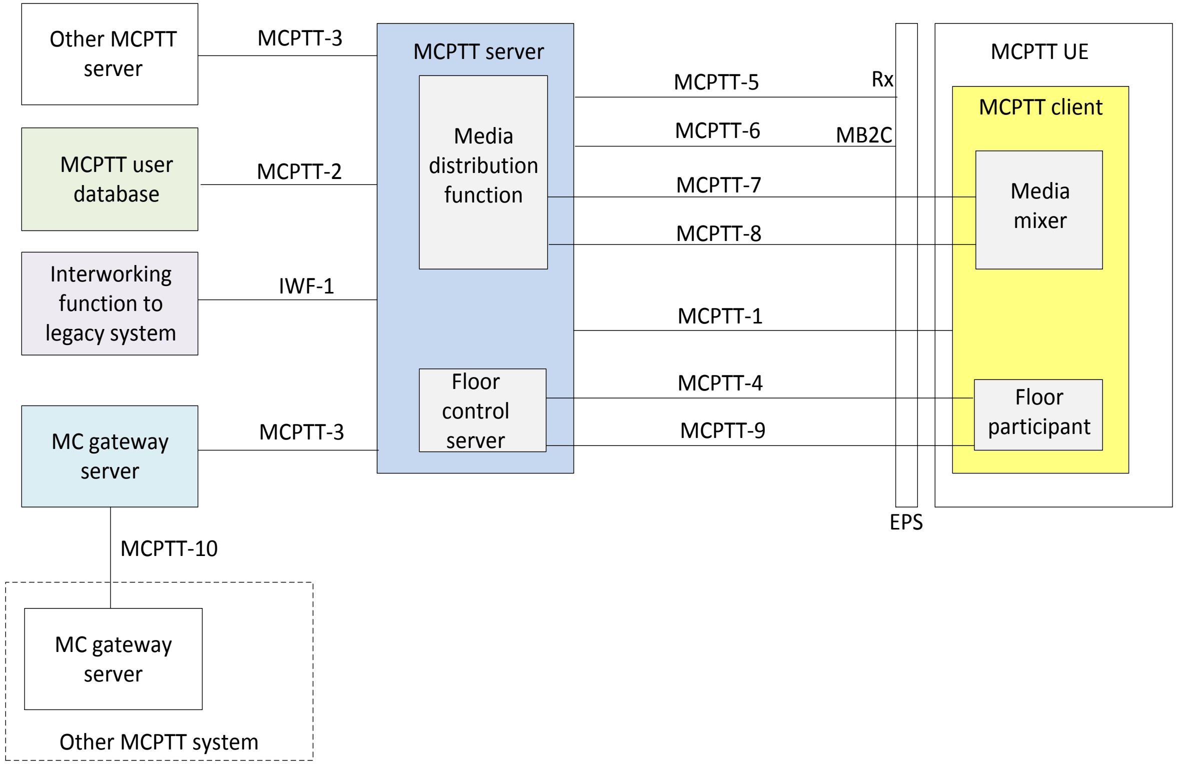
Mission Critical Push-To-Talk (MCPTT)

- The first Mission Critical service produced by SA6. MCPTT is one of the three pillars of Mission Critical services which provides real-time voice communications with a rich set of features to support Public Safety and other verticals (e.g. Railways).
  - Supports both private and group communications
  - Supports addressing, security, and priority that allows confidentiality from the network plane
  - Supports both unicast and multicast delivery of media and signalling, and off-network modes
- Key features
  - Affiliation and de-affiliation to groups
  - Manual and automatic commencement modes
  - Off-network utilizing ProSe and ProSe relay
  - Sophisticated group and user regrouping
  - Pre-established sessions
  - Emergency calls (private and group)
  - Imminent peril call, Emergency alert
  - Ambient listening
  - Floor priority and queuing
  - Functional alias management

MCPTT – Architecture

Key Functional Entities

- **MCPTT Client** includes Media Mixer and Floor Participant
- **MCPTT Server** includes Media Distribution Function and Floor Control Server
- **MCPTT User database** is the repository for user based capabilities
- **MCPTT Gateway server** is link to communication across MCPTT domains
- **Interworking Function** (IWF) is the link to LMR interoperability (and future GSM-R)



© 3GPP 2019

Mission Critical Video (MCVideo)

Purpose and Scope

- Mission critical video service using E-UTRAN access based on the common functional architecture for mission critical services and the EPC architecture.
- The MCVideo service can be used for public safety applications and also for general commercial applications e.g. utility companies and railways.

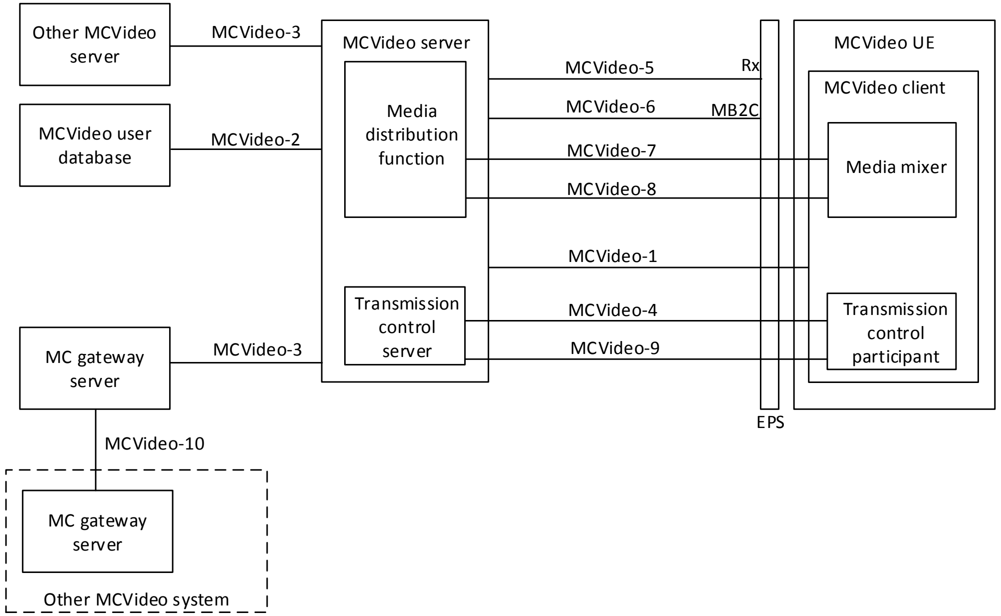
Key features

- Group communications
- Private communications
- Video Pull and Video Push
- Capability Information Sharing
- Ambient Viewing
- Transmission and Reception Control
- Supports high video resolution and enables license plate reading, facial and fingerprint recognition and overview of scenes
- Support for Low latency video modes (Emergency scenarios).
- Support high mobility

MCVideo – Architecture

Key Functional Entities

- Architecture entities developed utilizing CFA
- MCVideo server: Supports the MCVideo communications/services.
  - Media distribution function: Media handling (uplink, downlink, replication, storage, mixing.
  - Transmission control server: Controls media transmissions to UEs according to network situation and user intentions.
- MCVideo client: Supports the MCVideo transactions and remote device control.
  - Media mixer: sending and receiving one or multiple media streams and mixing.
  - Transmission control participant: Handling outgoing and incoming transmissions.



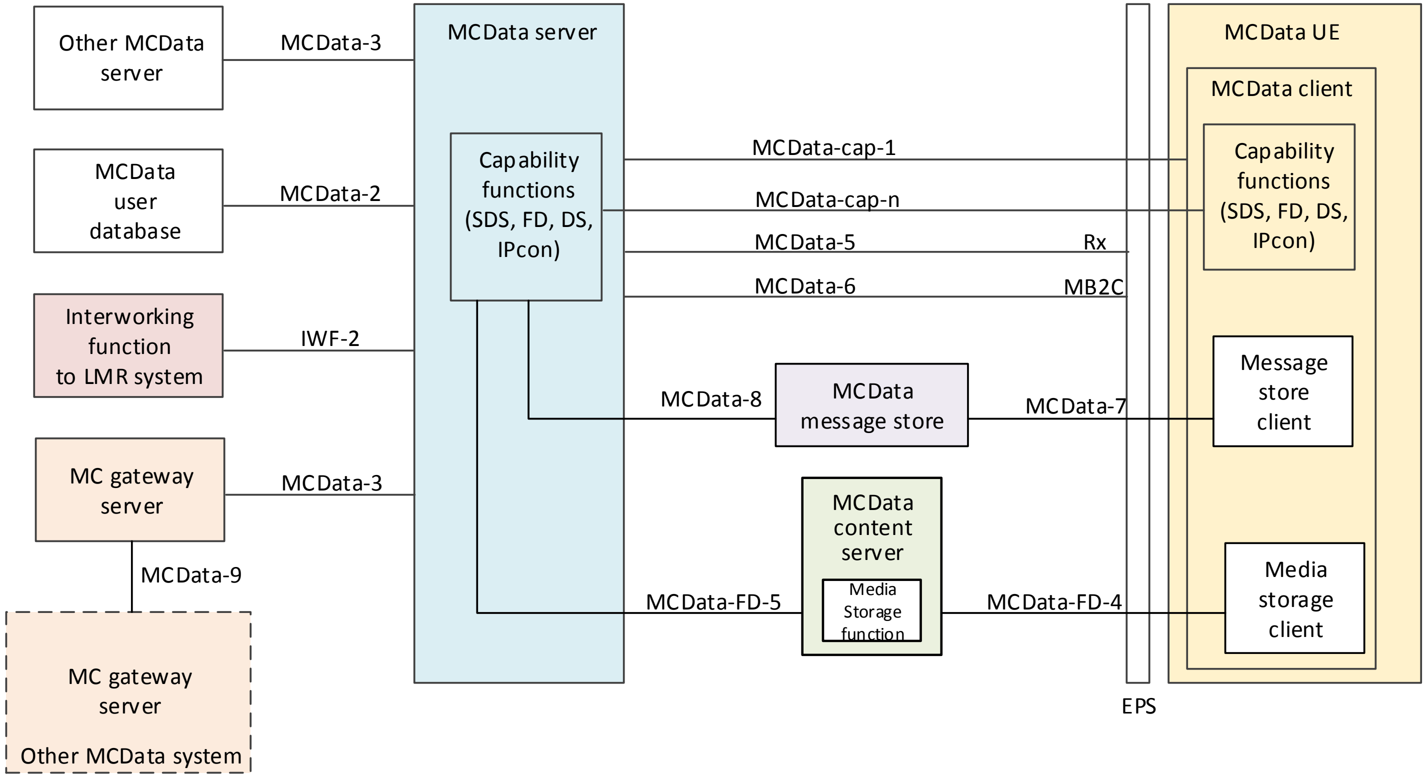
Mission Critical Data (MCData)

- One of the three pillars of the Mission Critical services that provides near real-time data communications
  - Support both private and group communications
  - Support both on and off network environment
  - Support both unicast and multicast delivery
- Key features
  - Short Data Service, using both signaling and media planes
  - File distribution, both for real-time and non real-time
  - Data streaming (planned for Rel-17)
  - IP connectivity
  - Conversation management
  - Transmission and reception control
  - Lossless communication
  - Network base message store
  - Regular and emergency services

MCData – Architecture

Key Functional Entities

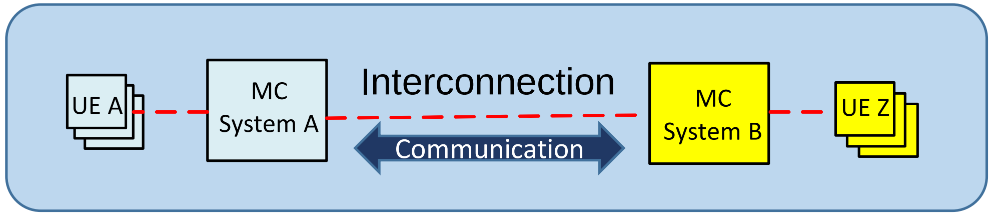
- MCData UE
- MCData Server
- MCData message store
- MCData content server
- Interworking function to LMR
- MC gateway server

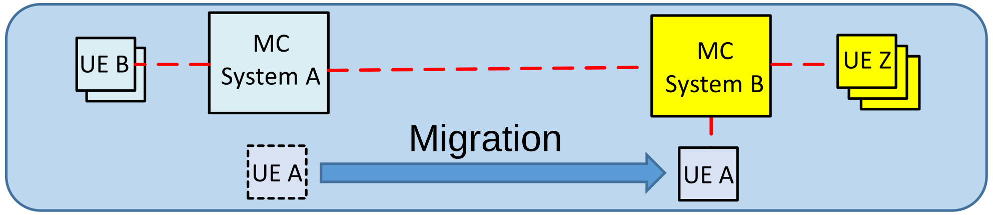


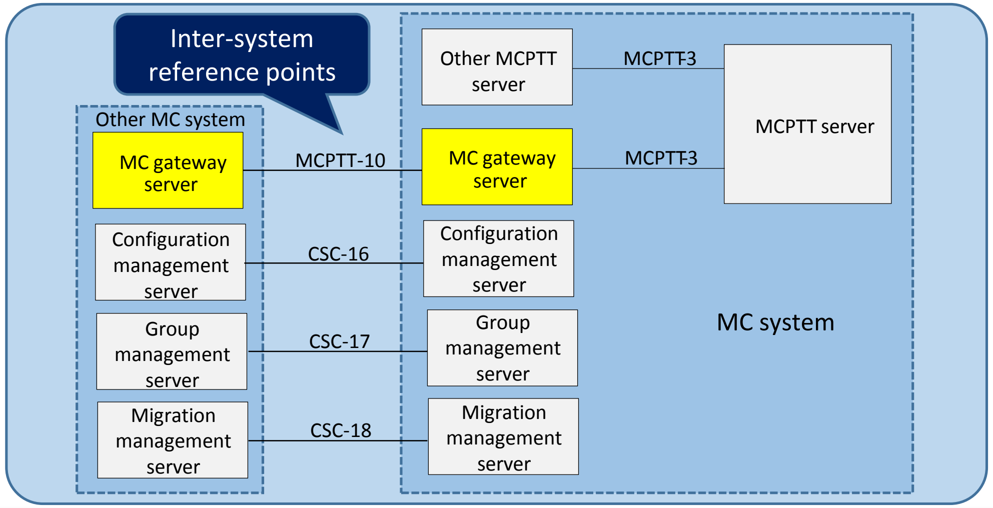
Mission Critical System Migration and Interconnection (MCSMI)

- Mission critical communication between users and groups in different MC systems that are in different security domains
  - National and international co-operation; mutual aid between states and territories etc
- Interconnection: calls to users and groups in partner MC systems
- Migration: obtaining service from partner MC systems

- Architectural elements
  - MC gateway server – provides topology hiding between MC systems
  - Configuration management: local MC system applies local rules to user and group configuration provided by partner MC system
  - Migration management – manages access information to partner MC system







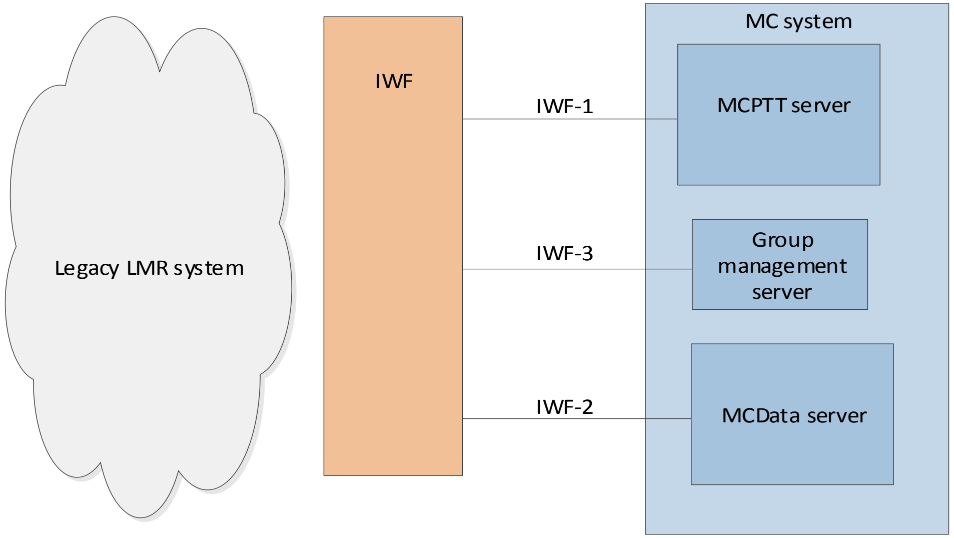
Mission Critical Communication Interworking (MCCI)

Purpose and Scope

- Adapts LMR (Land Mobile Radio, i.e. Public Safety radio) systems to MC systems
- The IWF (InterWorking Function), along with its LMR system, will appear as a peer interconnected MC system

Key features

- Group ‘affiliation’
- Group management / Regrouping
- Group calls / Private calls
- Broadcast calls / Emergency and imminent peril calls
- Short messaging
- Location
- Support for LMR end-to-end security



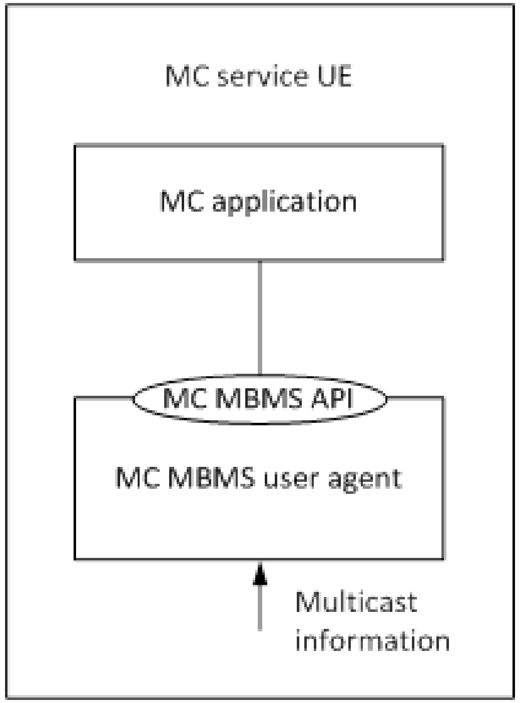
MC MBMS UE API (MBMSAPI_MCS)

Purpose and Scope

- Enables 3rd party Mission Critical Applications to access MBMS functionality on the UE

Key features

- Application registration/de-registration
- MBMS bearer registration/de-registration
- Get MBMS SAI/update notification
- Get cell info/update notification
- MBMS bearer notification
- Open/close media



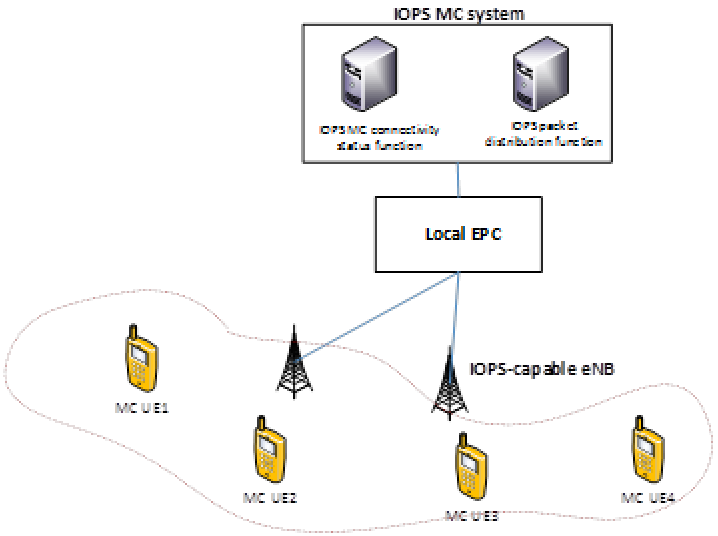
MC Over IOPS (FS_MCSAA)

Purpose and Scope

- This study focused on identifying application architecture solutions needed to support mission critical services during the Isolated E-UTRAN Operation for Public Safety (IOPS) mode of operation

Key features

- Solutions for the IOPS functional model and architectural model
- Solutions to address IOPS MC system synchronization aspects
- Potential application procedures to be utilized on the IOPS mode of operation


IOPS MC system
IOPS MC connectivity status function
IOPS packet distribution function
Local EPC
IOPS-capable eNB
MC UE1
MC UE2
MC UE3
MC UE4

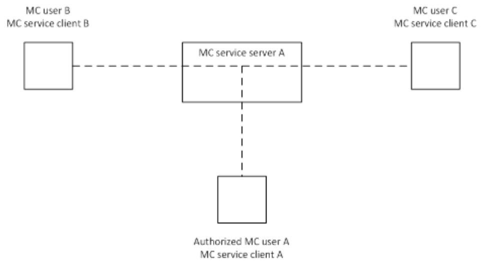
Discreet Listening & Logging (FS_MCLOG)

Discreet listening

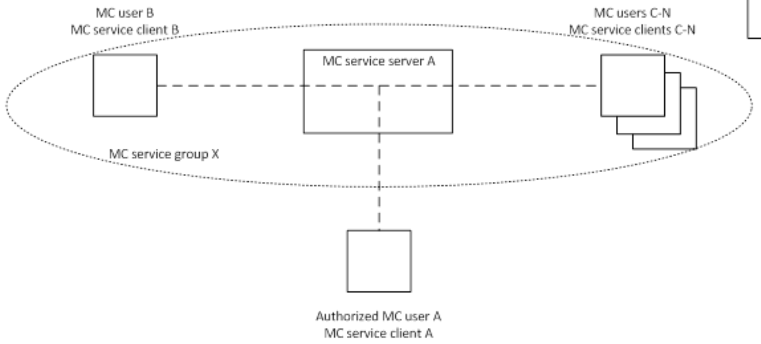
- MCPTT and MCVideo private calls
- MCPTT and MCVideo group calls
- MCVideo pull and push
- MCData SDS and file distribution

Logging

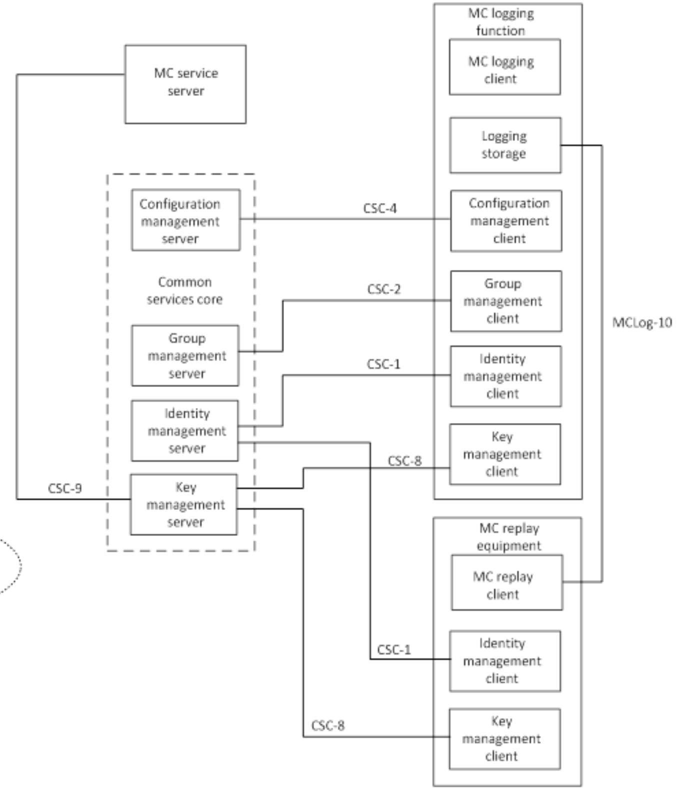
- MC logging function
- MC replay equipment



Private communication



Group Communication



Logging and Replay

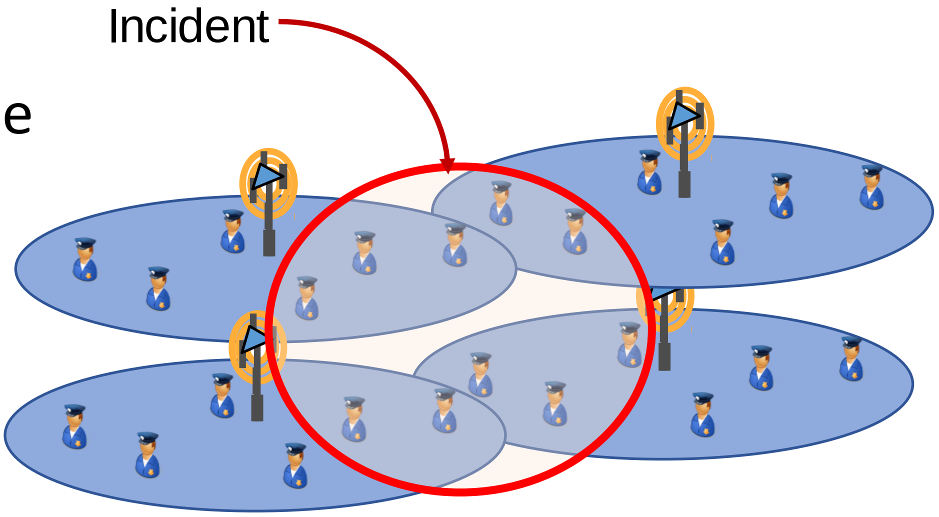
Location enhancements for MC services (FS_enhMCLoc)

Purpose and Scope

- This study focuses on identifying enhancements to the existing location architecture for MC services (MCPTT, MCVideo, MCData). These enhancements include such items as location history reporting and location of current talker.

Some key issues and solutions

- Location of a user logged into more than one device
- Location information in off-network operation
- Sharing of location information
- Triggering criteria in emergency scenarios
- Location accuracy including enhanced capabilities



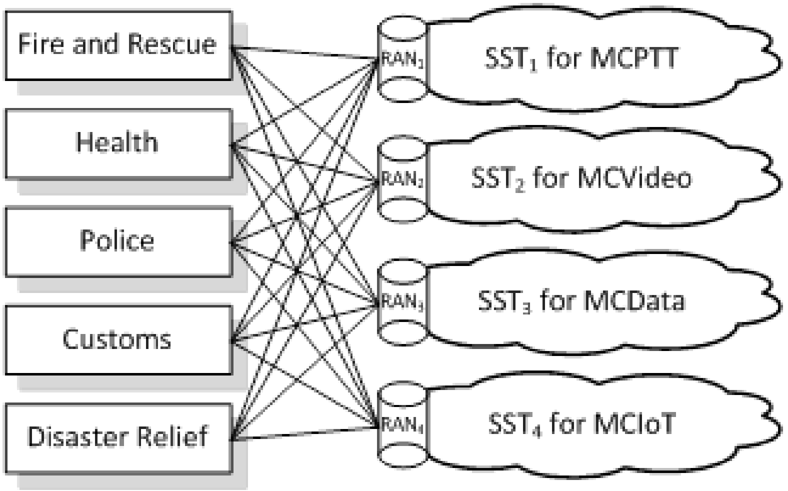
MC Services over 5G (FS_MCOver5GS)

Purpose and Scope

- To identify the impacts on and the necessary changes in the Stage 2 Mission Critical specifications to ensure that the set of Mission Critical services is supported over the 5GS

Aspects

- Terminology/textual changes
- Technical issues
  - Review and identify the 5GS aspects to support the Mission Critical architecture
    - Highlight missing 5GS features required for MC services
    - Use of new 5GS features
    - Impact of 5GS architecture



Outline

- Introduction to SA6
  - History and Evolution of SA6
  - Rel-16 / Rel-17 Overviews
- Mission Critical Topics
- Vertical Industry Enablement
- Conclusions

MONASTERY - Mobile Communication System for Railways

Purpose and Scope

- Enhance Mission Critical Communication by rail communication requirements to allow a migration from current GSM-R system towards FRMCS (Future Railways Mobile Communication System). The legacy GSM-R system will be not integral part of the FRMCS. Simply the focus is on interruptible service migration between GSM-R and FRMCS.

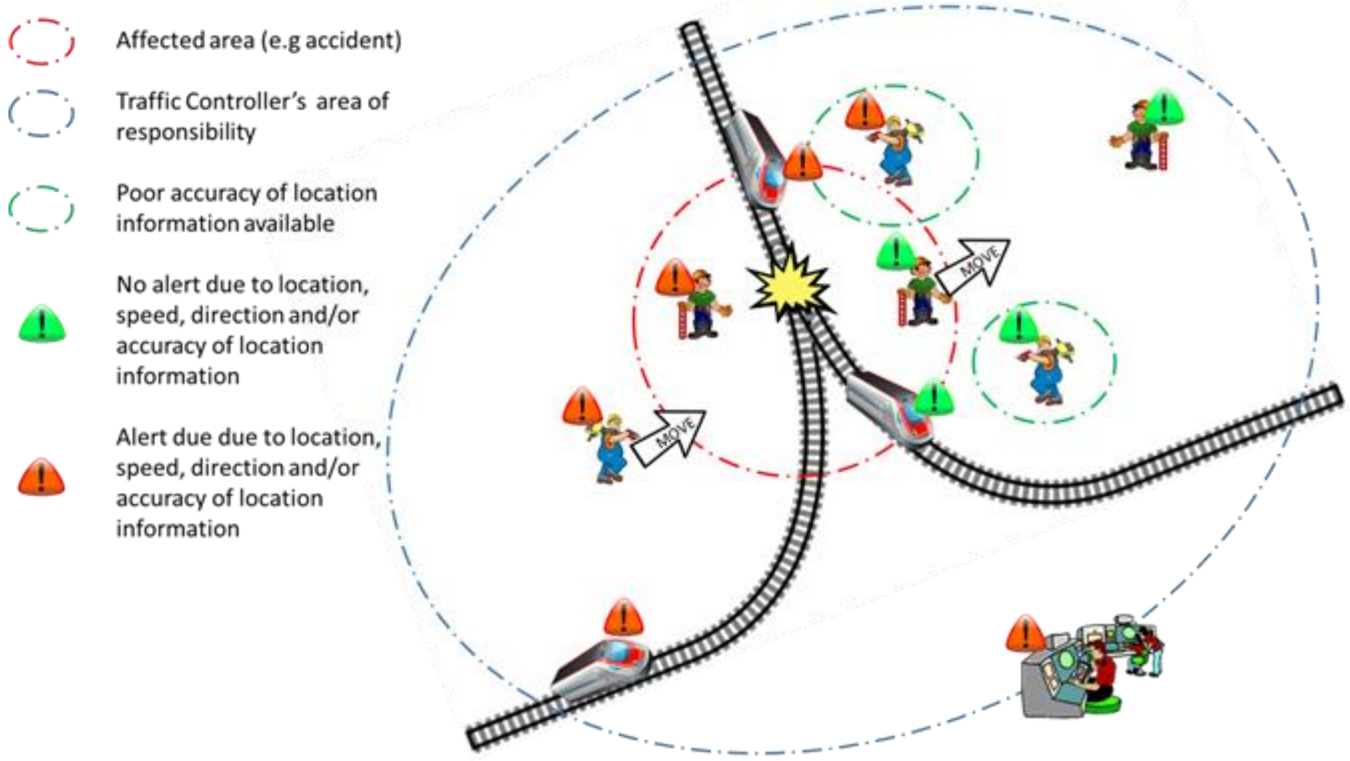
Key features

- Functional addressing of the user for operational purposes applicable for voice, video and data service types e.g. train number or current role of the user e.g. train driver;
- IP Connectivity for MC unaware data hosts e.g. train control command signalling (ETCS);
- Dynamic regrouping based on location and user roles;
- Specific railway functions for private and group communications (call forwarding, affiliation based on functional address etc.)
- Interworking with GSM-R;
- Sharing of one UE by multiple users simultaneously (Gateway UE).

MONASTERY – High Level Services

Key railway communication services

- Operational role management
- Multi-Talker control in group communication
- Location dependent communication
- IP connectivity for safety and non-safety rail applications
- Maintenance services (location based grouping)
- Railway specific services like railway emergency calls/alerts, location-dependent communication
- Interworking with legacy GSM-R



Affected area (e.g accident)

Traffic Controller's area of responsibility

Poor accuracy of location information available

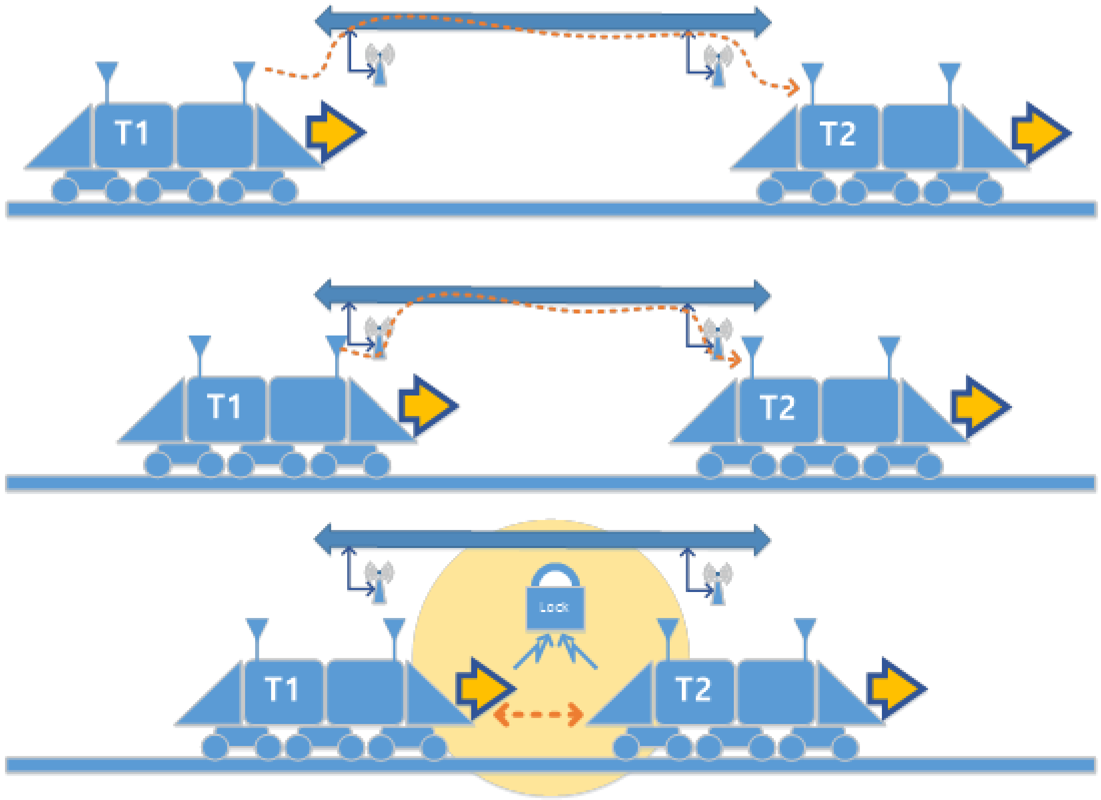
No alert due to location, speed, direction and/or accuracy of location information

Alert due due to location, speed, direction and/or accuracy of location information

MONASTERY – High Level Services (2) for further study

Key railway communication services

- Interworking between MCX system using functional addressing
- Off-network communication for virtual coupling and train integrity
- Gateway UE



Common API Framework (CAPIF)

Purpose and Scope

- During Release 15, the Common API Framework (CAPIF) was developed to enable a unified Northbound API framework across 3GPP network functions, and to ensure that there is a single and harmonized approach for API development (Refer to 3GPP TS 23.222, TS 33.122 and TS 29.222).
- CAPIF provides a framework to host network and service APIs of PLMN and from 3rd party domain.
- This work has been successfully delivered and integrated with Northbound APIs developed by 3GPP SA2 Working Group (SCEF/NEF) and 3GPP SA4 (xMB).

Key features

- On-boarding/off-boarding API invoker
- Register/de-register APIs
- Discovery of APIs
- CAPIF events Subscription/Notification
- Entity Authentication/Authorization
- Enables secure communication
- Support for 3rd party domains i.e. to allow 3rd party API providers to leverage the CAPIF framework
- Support for interconnection between two CAPIF providers
- The federation of CAPIF functions to support distributed deployments.

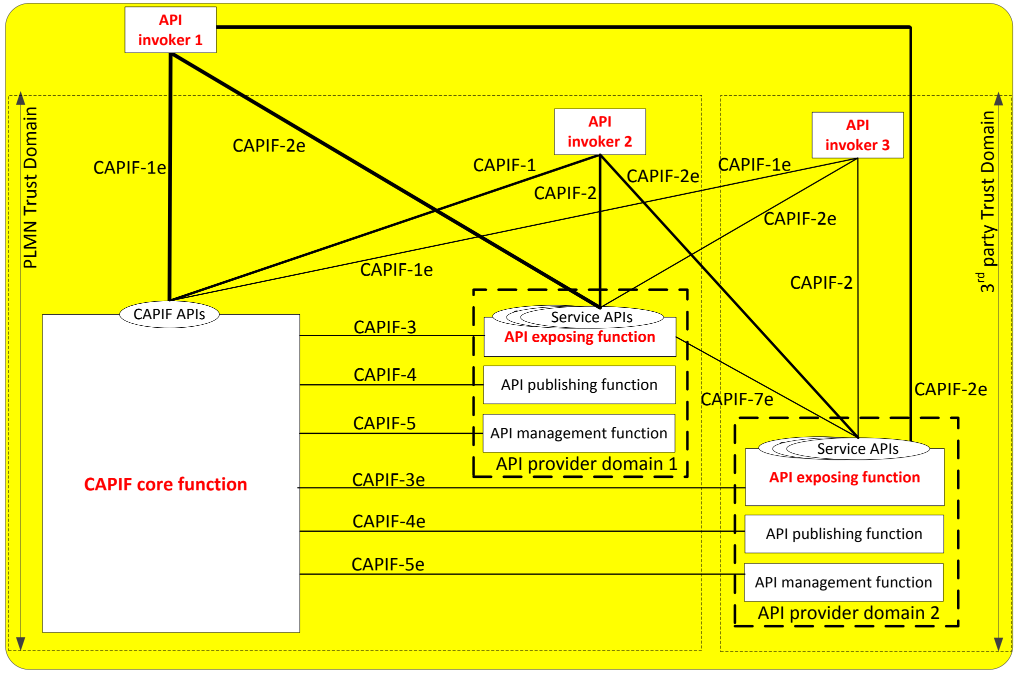
CAPIF – Architecture

Key Functional Entities

- **CAPIF Core Function (CCF)** is a repository of all, PLMN and 3rd party, service APIs
  - allows discovery of the stored APIs by the API invokers and AEFs
  - authenticates and authorizes API invokers for use of the service APIs
  - logging and charging the API invocations

- **API Exposing Function (AEF)** is the provider of the services as APIs
  - validates the authorization of the API Invokers
  - provides the service to the API invoker
  - logs the invocations on the CCF and requests charging for the service.

- **API Invoker** is typically the applications that require service from the service providers
  - discovers the service APIs from the CAPIF Core Function
  - seeks authorization for API invocations
  - avails the services provided by the AEFs



Functional model for the CAPIF to support 3rd party API providers

Service Enabler Architecture Layer for Verticals (SEAL)

Purpose and Scope

- 3GPP networks witnessing increasing demand from various vertical industries
- It is apparent that vertical applications will require similar core capabilities in a timely manner
- 3GPP Release 16 TS 23.434 specifies application-enabling services that can be reused across vertical applications (e.g. V2X applications)
- SEAL also specifies the northbound APIs (complaint with CAPIF) - to enable flexible integration with vertical applications.

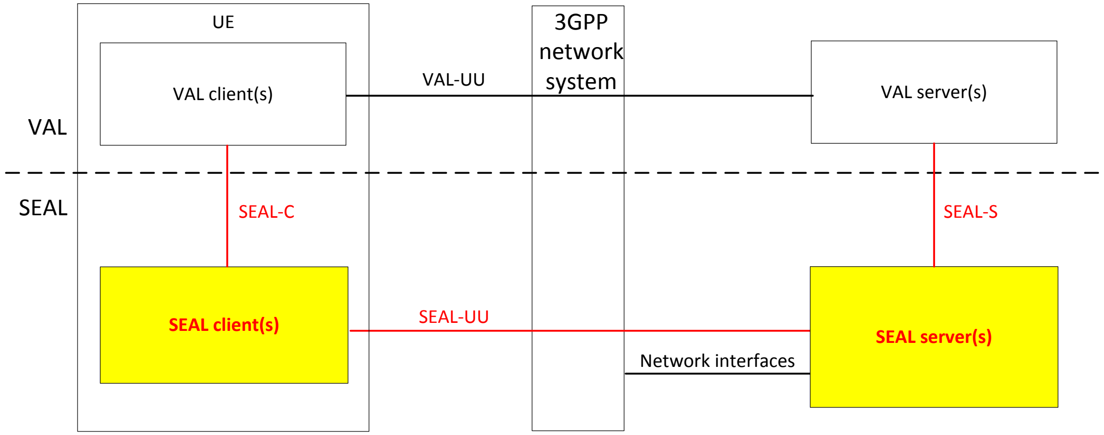
Key features

- SEAL services include
  - Group management
  - Configuration management
  - Location management
  - Identity management
  - Key management
  - Network resource management
- SEAL services are supported both in on-network and off-network
- Interconnection between SEAL servers to support distributed SEAL server deployments
- Inter-service communication between SEAL servers (e.g. location based group management)

SEAL – Architecture

Key Functional Entities

- **SEAL client** (client side functionalities corresponding to the specific SEAL service)
  - supports interactions with the VAL client(s) and with the corresponding SEAL client between the two UEs
- **SEAL server** (server side functionalities corresponding to the specific SEAL service)
  - supports interactions with the VAL server(s) and with the corresponding SEAL server in distributed SEAL deployments
  - acts as CAPIF's API exposing function (AEF)



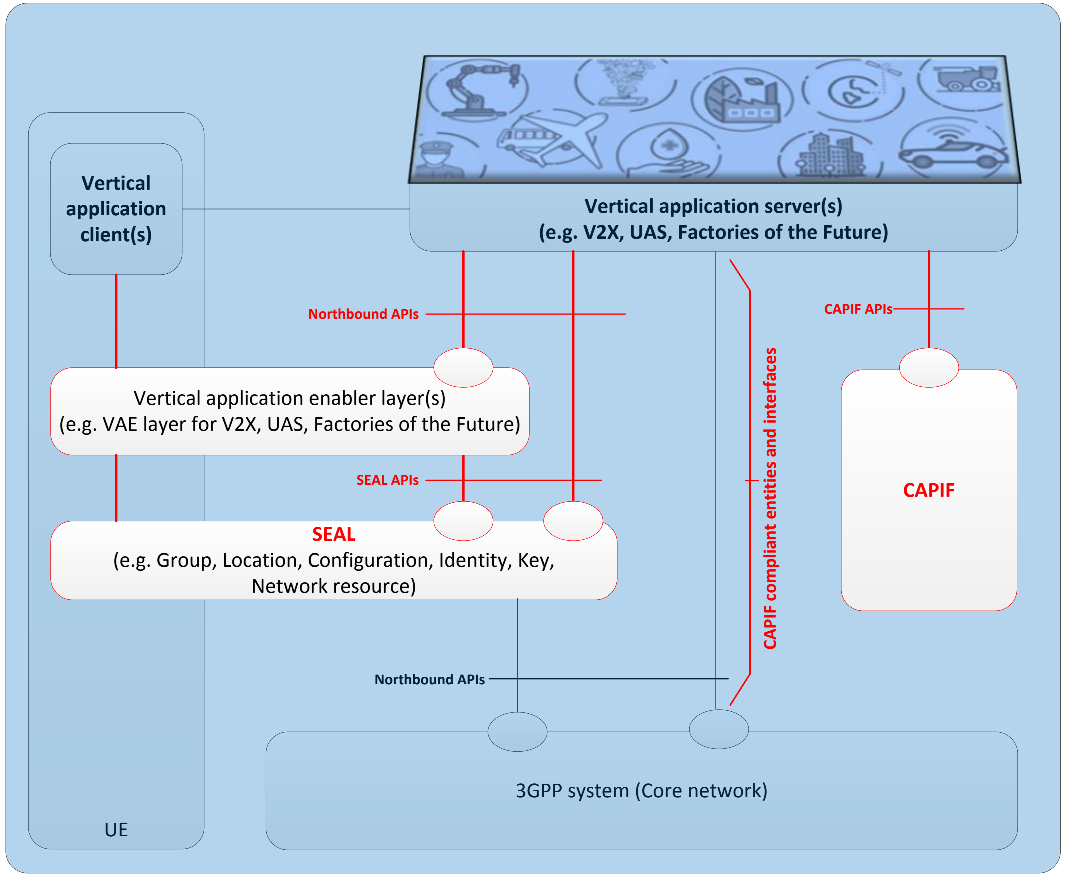
Generic on-network functional model

Leveraging CAPIF and SEAL

- Enables rapid deployment of new vertical applications, with access to the common SEAL services provided by MNOs:
  - **SEAL** services (e.g. location, group, etc.) are exposed as Northbound APIs
  - **CAPIF** is used for publishing and discovery of SEAL services by the Vertical applications

Benefits

- Vertical Service Provider – reduced time to market
- Network Operator – maximize reuse of their existing deployments


Vertical application client(s)
Vertical application server(s)
(e.g. V2X, UAS, Factories of the Future)
Northbound APIs
CAPIF APIs
Vertical application enabler layer(s)
(e.g. VAE layer for V2X, UAS, Factories of the Future)
SEAL APIs
SEAL
(e.g. Group, Location, Configuration, Identity, Key, Network resource)
CAPIF compliant entities and interfaces
CAPIF
Northbound APIs
3GPP system (Core network)
UE

© 3GPP 2019

V2X Application (V2XAPP)

Purpose and Scope

- V2X application enabler layer that is necessary to ensure efficient use and deployment of V2X services over 3GPP systems.
- Currently supports EPS. Study ongoing to support 5GS.

Key features

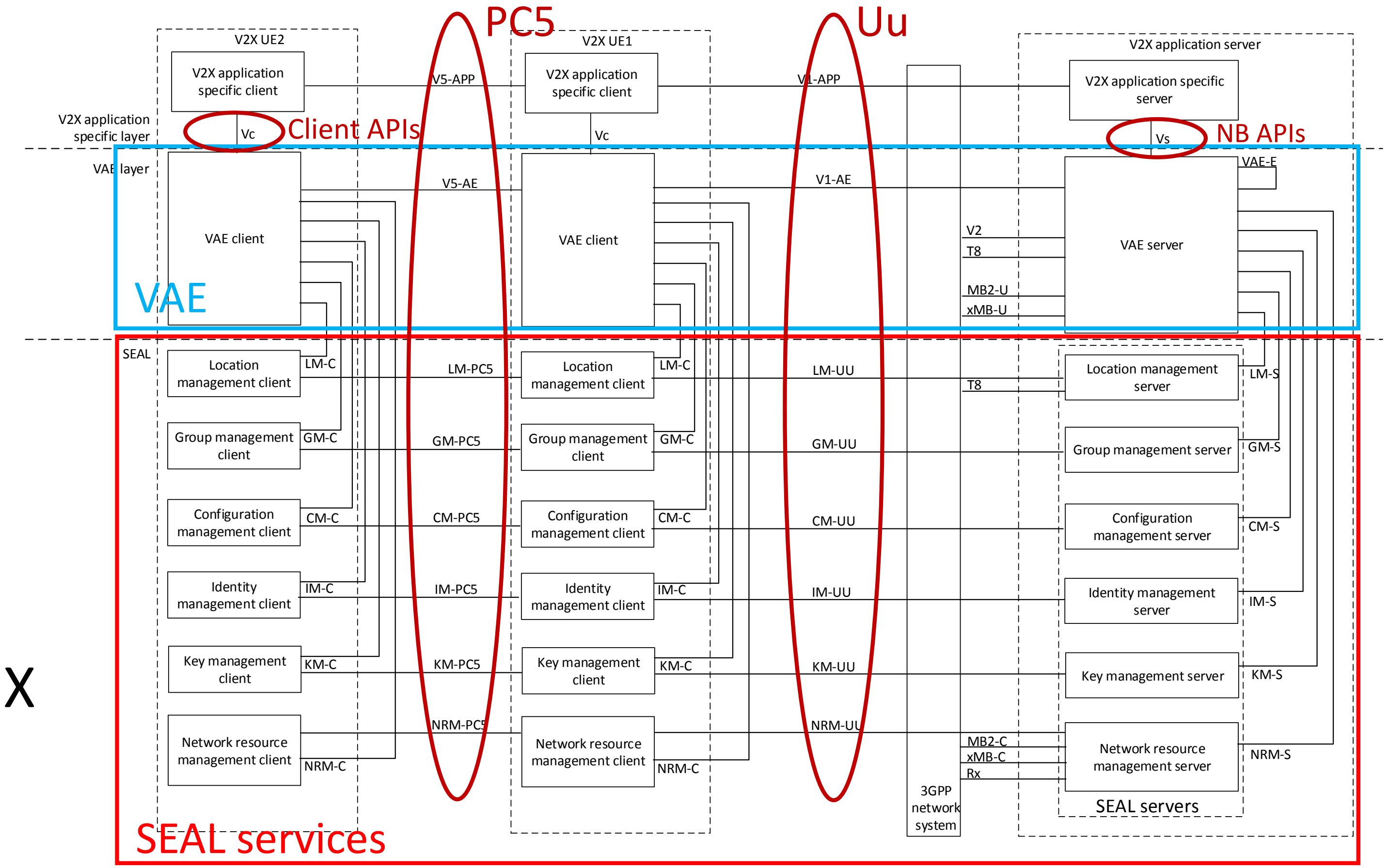
- V2X service discovery
- Application level location tracking
- V2X message delivery
- File distribution
- Provisioning 3GPP system info

- Network monitoring
- V2X application resource management
- Dynamic group management (platooning support)
- V2X service continuity

V2XAPP – Architecture

- V2X application architecture developed based on SEAL.

- Key Functional Entities
  - VAE client and server: Abstracts the common V2X support functions and user plane interactions with 3GPP network systems. Provides APIs to the V2X application specific functions


PC5
Uu
V2X UE2
V2X UE1
V2X application server
V2X application specific client
V2X application specific client
V2X application specific server
V2X application specific layer
VAE layer
SEAL
Vc
Vc
Vs
Client APIs
NB APIs
V5-APP
V1-APP
V5-AE
V1-AE
VAE-E
VAE client
VAE client
VAE server
V2
T8
MB2-U
xMB-U
VAE
Location management client
Location management client
Location management server
LM-C
LM-PC5
LM-UU
LM-S
T8
Group management client
Group management client
Group management server
GM-C
GM-PC5
GM-UU
GM-S
Configuration management client
Configuration management client
Configuration management server
CM-C
CM-PC5
CM-UU
CM-S
Identity management client
Identity management client
Identity management server
IM-C
IM-PC5
IM-UU
IM-S
Key management client
Key management client
Key management server
KM-C
KM-PC5
KM-UU
KM-S
Network resource management client
Network resource management client
Network resource management server
NRM-C
NRM-PC5
NRM-UU
NRM-S
MB2-C
xMB-C
Rx
3GPP network system
SEAL servers
SEAL services

Edge Application (EDGEAPP)

Purpose and Scope

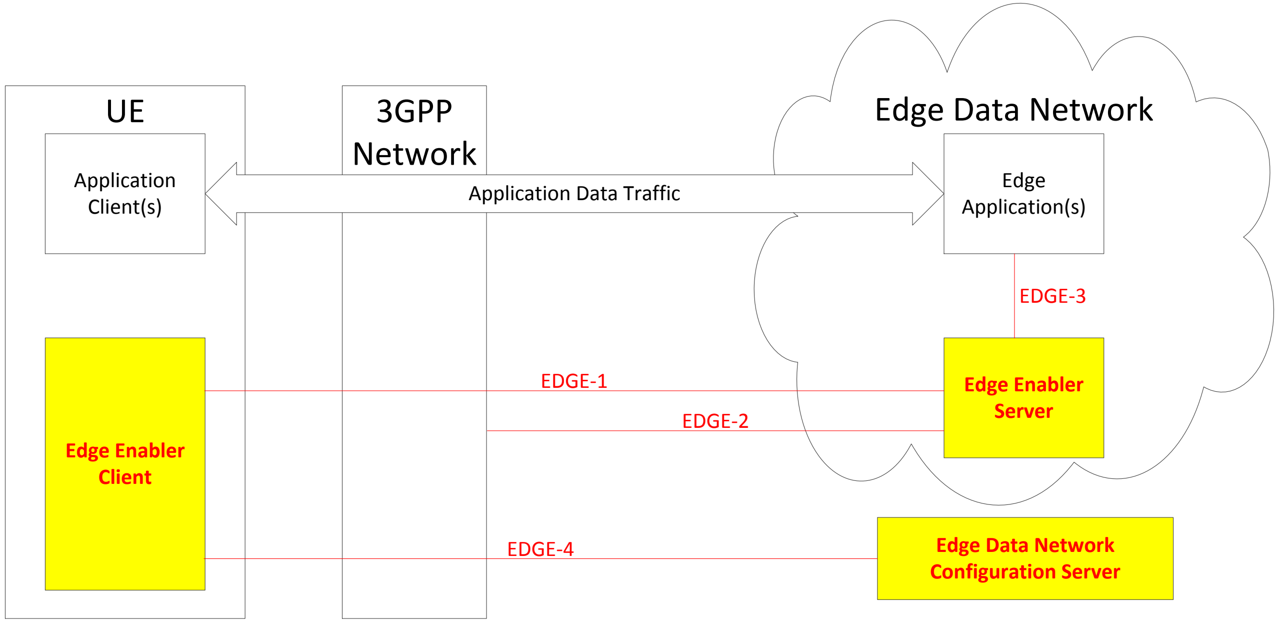
- Edge Computing in 3GPP will help achieve the performance goals of Verticals, providing **low latency and massive broadband**.
- The study aims to define a **supporting application layer**, which enables the deployment of applications on the edge of 3GPP networks, with **minimal impacts to edge-based applications** on the UE.

Key features

- **UE application portability** Changes in Application Clients compared to existing cloud environment are avoided.
- **Edge application portability** Changes in Application Servers compared to existing cloud environment are avoided.
- **Service differentiation** The mobile operator is able to provide service differentiation (e.g. by enabling/disabling the Edge Computing functionalities).
- **Flexible deployment** There can be multiple Edge Computing providers within a single PLMN operator network. The Edge Data Network can be a subarea of a PLMN.
- **Interworking with 3GPP network** Capability exposure, such as location service, QoS, AF traffic influence, to the Edge Applications.
- **Service continuity** Support for continuation of application context across Edge deployments

EDGEAPP – Architecture

- Key Functional Entities
  - **Edge Enabler Server:** Provides information related to the Edge Applications, such as availability and related configuration, to the Edge Enabler Client; and exposes capabilities of 3GPP network to Edge Applications.
  - **Edge Enabler Client:** Enables discovery of Edge Applications and provisioning of configuration data
  - **Edge Data Network Configuration Server:** Providing Edge Data Network configuration information to the Edge Enabler Client



Application architecture for enabling edge applications

- The study report is being documented in 3GPP TR 23.758, and is expected to be complete by December’2019.

Factories of the Future Application (FFAPP)

- FFAPP identifies architecture requirements and application architecture to ensure efficient use and deployment of application layer support for Factories of the Future in 5G network.
  - takes into consideration the existing work including stage 1 requirements in 3GPP TS 22.261 and 3GPP TS 22.104, and provides recommendation for normative work
- Key features
  - support for network slicing, cross network slice coordination
  - Geographic location and positioning information support
  - clock synchronization, TSN supporting
  - QoS monitoring, Managing non-public network
  - 5GLAN group management

FFAPP – Architecture

- Key Functional Entities
  - Not yet design
- Other Areas of Interest
  - alliance with 5G-ACIA White Paper – **5G Network Exposure Interface for Enterprises**

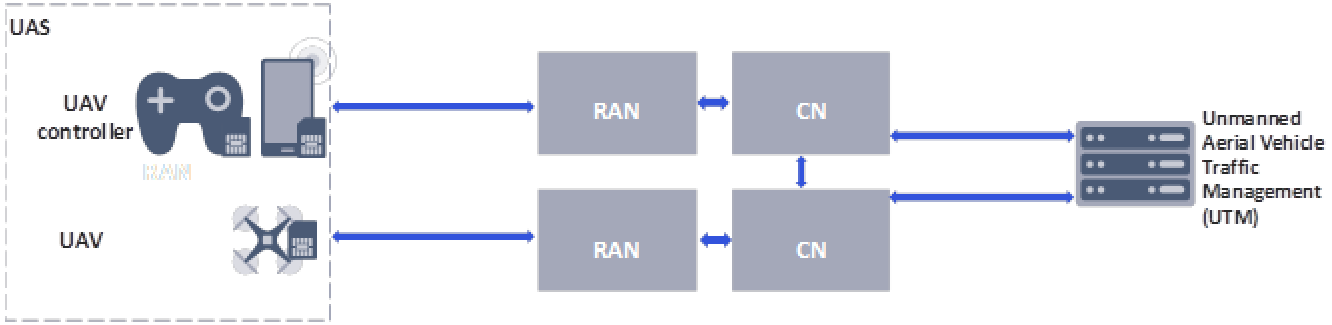
Unmanned Aerial System Application (UASAPP)

Purpose and Scope

- Identify the application aspects to support UAS that are necessary to ensure efficient use and deployment of UAS services and applications over 3GPP systems.

Key features

- Authentication and authorization
- UTM command communication
- Location tracking
- ….



Study is in progress

Outline

- Introduction to SA6
  - History and Evolution of SA6
  - Rel-16 / Rel-17 Overviews
- Mission Critical Topics
- Vertical Industry Enablement
- Conclusions

Conclusions

- 3GPP has established a mature set of MCX standards
  - Enhancements will continue!
- Expanded SA6 scope has enabled standardized support for vertical industries
- Industry feedback is critical to robust standards
  - ETSI Mission Critical Plugtests™
  - Additional input through requirements and liaisons
- Participation is essential: Please join us
  - Contribution-driven approach – Your voice will be heard!

Thank you for your attention!

info@3gpp.org
s.chitturi@samsung.com

www.3gpp.org

Search for WIDs at http://www.3gpp.org/specifications/work-plan and http://www.3gpp.org/ftp/Information/WORK_PLAN/