3GPP SA6 initiatives to enable new vertical applications

Suresh Chitturi

3GPP SA6 Chairman

© 3GPP 2019

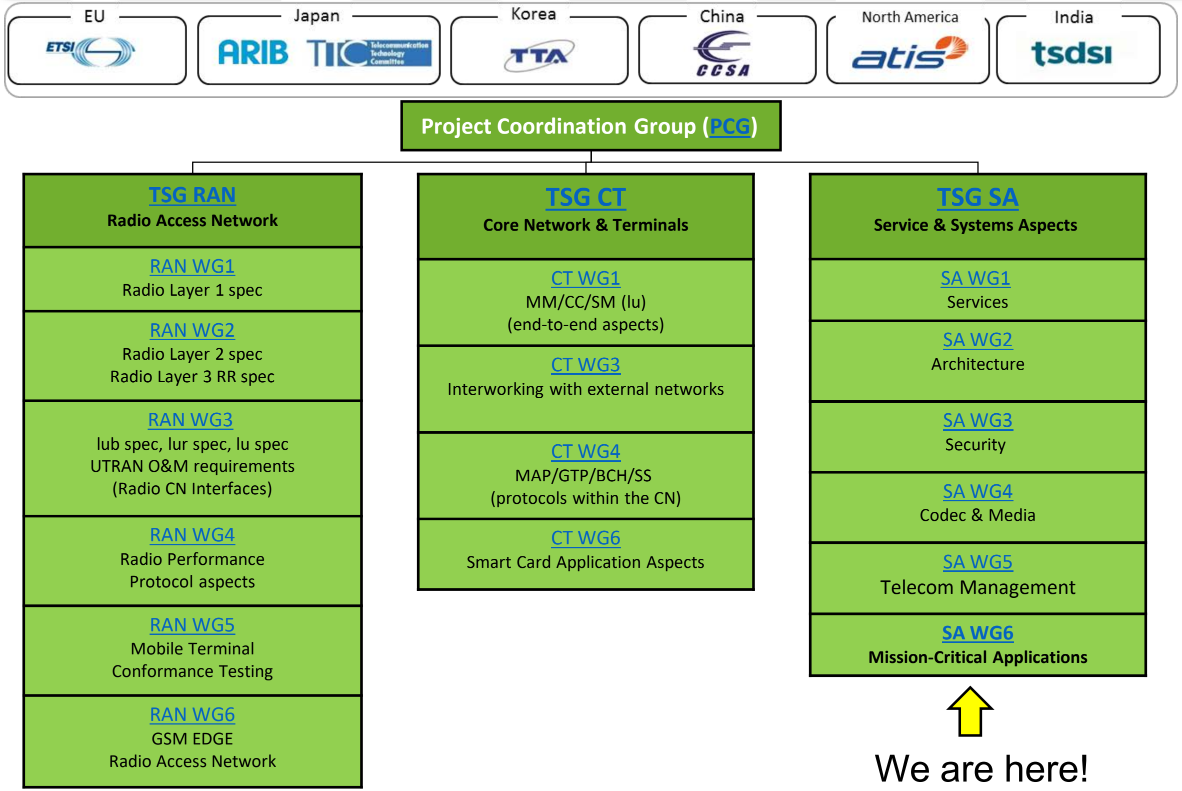
Outline

- Introduction to 3GPP SA6
- Why SA6 is important for 5G Verticals
- Key vertical application initiatives in SA6
  - MCX – Mission Critical Services
  - CAPIF – Common API Framework
  - SEAL – Service Enabler Architecture Layer
  - EDGEAPP – Application Architecture for Edge Applications
- Future work on verticals
- Summary

© 3GPP 2019

3GPP Organization Structure

3GPP
A GLOBAL INITIATIVE



EU: ETSI | Japan: ARIB TTC | Korea: TTA | China: CCSA | North America: atis | India: tsdsi

Project Coordination Group (PCG)

TSG RAN
Radio Access Network

- RAN WG1 — Radio Layer 1 spec
- RAN WG2 — Radio Layer 2 spec, Radio Layer 3 RR spec
- RAN WG3 — lub spec, lur spec, lu spec, UTRAN O&M requirements (Radio CN Interfaces)
- RAN WG4 — Radio Performance Protocol aspects
- RAN WG5 — Mobile Terminal Conformance Testing
- RAN WG6 — GSM EDGE Radio Access Network

TSG CT
Core Network & Terminals

- CT WG1 — MM/CC/SM (lu) (end-to-end aspects)
- CT WG3 — Interworking with external networks
- CT WG4 — MAP/GTP/BCH/SS (protocols within the CN)
- CT WG6 — Smart Card Application Aspects

TSG SA
Service & Systems Aspects

- SA WG1 — Services
- SA WG2 — Architecture
- SA WG3 — Security
- SA WG4 — Codec & Media
- SA WG5 — Telecom Management
- **SA WG6 — Mission-Critical Applications**

We are here!

- 3GPP – The 3rd Generation Partnership Project ("the project")
- PCG – Coordination of 3GPP by the Organizational Partners (OPs)
- Technical Specification Groups (TSGs) covering different aspects of 3GPP system & process
- TSGs are organized into Working Groups (WGs)
- TSGs meet 4 times a year in the so-called "Plenary meetings" (co-located)
- WGs meet once or more per plenary cycle (mostly not co-located)
- Each TSG and each WG elects its own leadership (2 year terms / 2 terms)
- Technical work is mostly done in WGs
- Overall planning and coordination in TSGs

© 3GPP 2019

SA6 Leadership Team

Suresh Chitturi
SA6 Chairman
TTA
s.chitturi@samsung.com

Alan Soloway
SA6 Vice-Chairman
ATIS
asoloway@qti.qualcomm.com

Bernt Mattsson
Secretary
MCC
bernt.mattsson@etsi.org

Jukka Vialen
SA6 Vice-Chairman
ETSI
jukka.vialen@airbus.com

© 3GPP 2019

Companies engaged in SA6

*** Non-exhaustive**

3GPP
A GLOBAL INITIATIVE

Mission Critical

- astrid
- BDBOS
  digital . sicher . bundesweit
- FirstNet
- Home Office
- ERILLISVERKOT
- SBB CFF FFS
- POLITIE

Operators

- at&t
- SK telecom
- 中国移动 China Mobile
- TELECOM ITALIA
- China unicom中国联通
- sysoco Wireless technology
- Deutsche Telekom
- TELSTRA
- verizon
- kapsch
- vodafone

Vendors

- AIRBUS
- BULL
- NOKIA
- SOFTIL
  INNOVATIVE COMMUNICATIONS
- BlackBerry
- HUAWEI
- ONE2MANY
- SONY
- L3HARRIS
- intel
- ERICSSON
- tait communications
- sepura
- Qualcomm
- TD Tech
- ENENSYS
- EXPWAY
- SAMSUNG
- Tencent腾讯
- PHILIPS
- LG
- ZTE中兴

Researchers

- CATT
- सत्यमेव जयते
  Department of Telecommunications
- KRRI
- Fraunhofer
- 한성대학교 HANSUNG UNIVERSITY
- iit delhi
- IIT Hyderabad
- nomor research novel mobile radio

© 3GPP 2019

Why SA6 is important for 5G Verticals

- Does each vertical want to create its own solution for each service?
    - Management of groups, location, identity, keys, configurations, network resources
- Does each vertical want to negotiate with each MNO on how best to utilize network resources?
- Does each vertical want to convince each MNO to use its defined API interface?
- Does each application developer want to adapt to each required MNO API interface?
- Does each private 5G deployment want to negotiate and adapt to each infrastructure provider?
- Does each infrastructure provider want to negotiate and adapt to each private 5G deployment?

We need a middleware layer and common services to simplify the implementation and deployment of vertical systems at large scale.

© 3GPP 2019

MCX - Mission Critical Standards

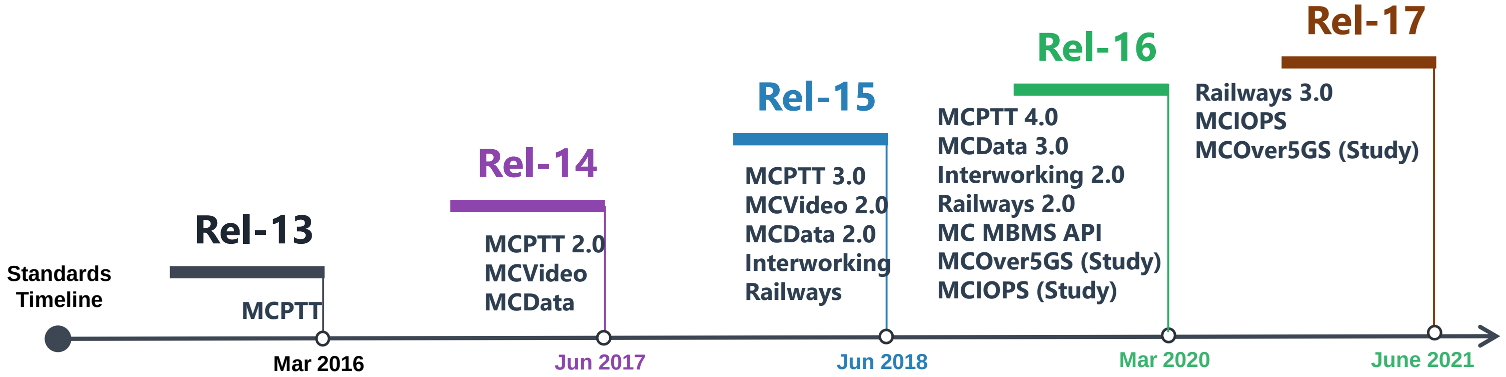
TS 23.379 [MCPTT] TS 23.281 [MCVideo] TS 23.282 [MCData] TS 23.280 [CFA]

MC standardization was initiated in 2013

- Initiated by public safety agencies of Korea, USA, UK, France, Germany, Netherlands, and TCCA, ETSI, ATIS, TTA

3GPP identified as the home for global Mission Critical Services (MCX) Standards

- Over 600 user requirements were developed 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) and it continues…



Standards Timeline

Rel-13
MCPTT
Mar 2016

Rel-14
MCPTT 2.0
MCVideo
MCData
Jun 2017

Rel-15
MCPTT 3.0
MCVideo 2.0
MCData 2.0
Interworking
Railways
Jun 2018

Rel-16
MCPTT 4.0
MCData 3.0
Interworking 2.0
Railways 2.0
MC MBMS API
MCOver5GS (Study)
MCIOPS (Study)
Mar 2020

Rel-17
Railways 3.0
MCIOPS
MCOver5GS (Study)
June 2021

© 3GPP 2019

Common API Framework (CAPIF)

TS 23.222

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.

© 3GPP 2019

CAPIF – Architecture

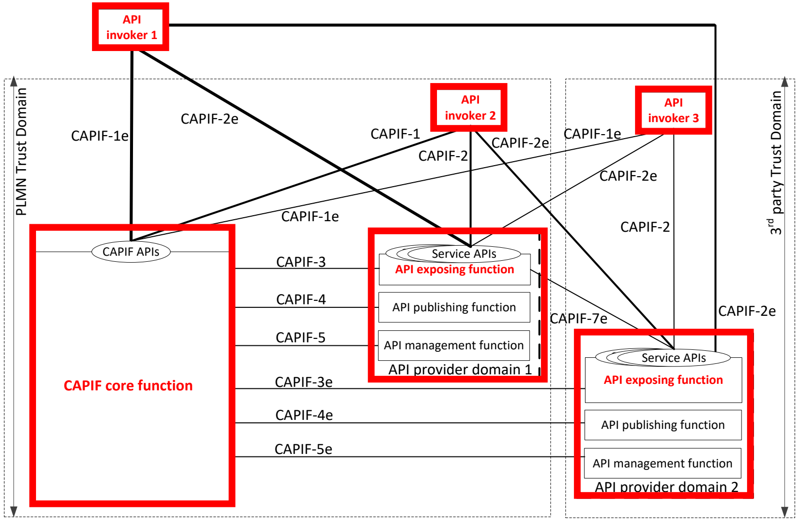
TS 23.222

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

© 3GPP 2019

Service Enabler Architecture Layer (SEAL)

TS 23.434

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)

© 3GPP 2019

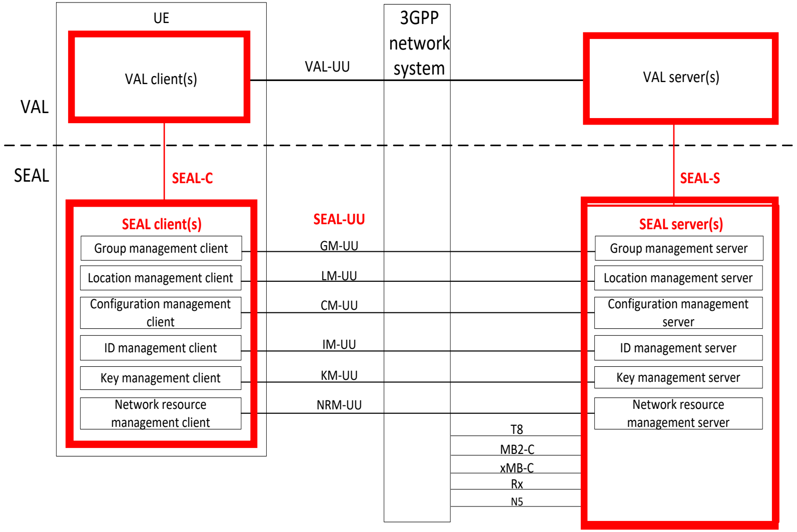
SEAL – Architecture

TS 23.434

Key Functional Entities

- **SEAL client(s)** - 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 (s)** - 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)

VAL – Vertical Application Layer e.g. V2X app



Functional model

© 3GPP 2019

Application Architecture for Edge Apps (EDGEAPP)

TR 23.758

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.

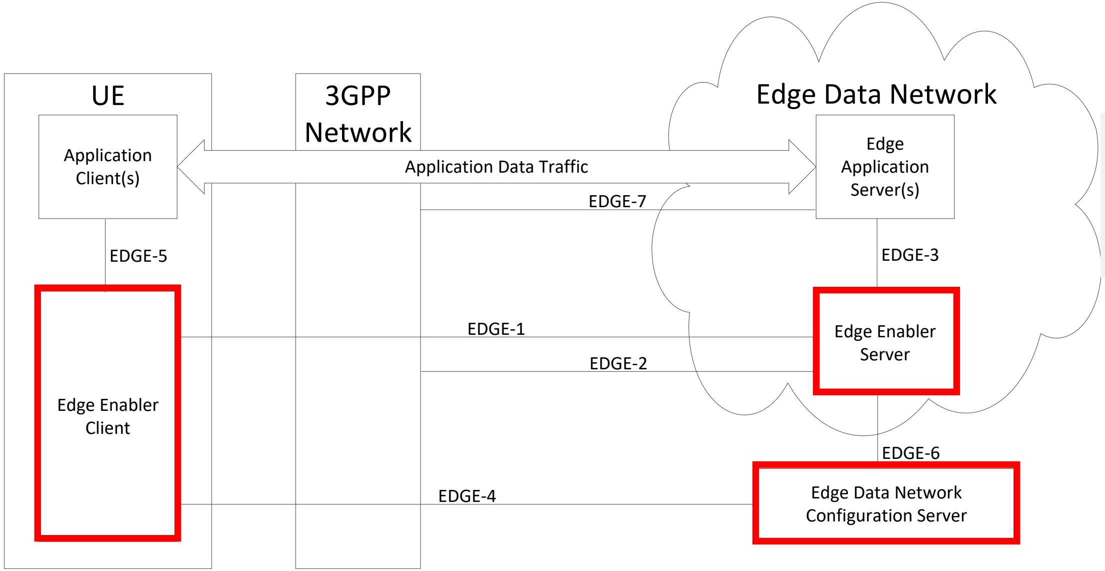
Key Requirements

- **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.
- **Integration w/3GPP network** Capability exposure, such as location service, QoS, AF traffic influence, to the Edge Apps.
- **Service continuity** Support for continuation of application context across Edge deployments

© 3GPP 2019

EDGEAPP – Application Architecture

TR 23.758



- **Edge Enabler Client:** Enables discovery of Edge Applications and provisioning of configuration data

- **Edge Enabler Server:** Provides information related to the Edge Applications, such as availability/enablement and related configuration, to the Edge Enabler Client; and exposes capabilities of 3GPP network to Edge Applications.

- **Edge Data Network Configuration Server:** Providing Edge Data Network configuration information to the Edge Enabler Client

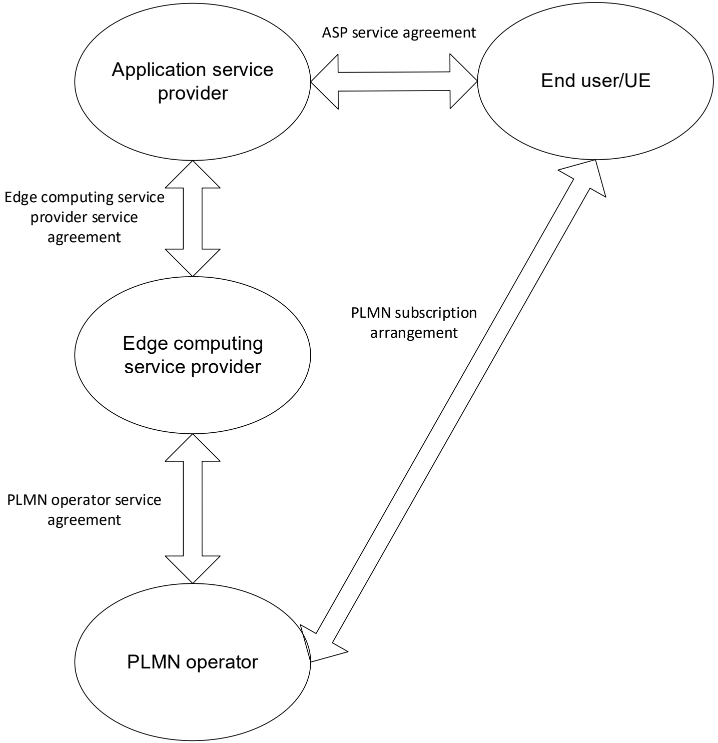
© 3GPP 2019

EDGEAPP – Business Relationships

TR 23.758

- **End user** is the consumer of the applications provided by the ASP.
  - service agreement with a single or multiple ASP(s).
  - a PLMN subscription with the PLMN operator.
- The **ASP** consumes the edge services (e.g. infrastructure, platform) provided by the ECSP.
  - service agreement with a single or multiple ECSP(s).
- The **ECSP** has service agreement with single or multiple PLMN operators or both are part of the same organization.

ASP: Application Service Provider; **ECSP:** Edge Computing Service Provider;

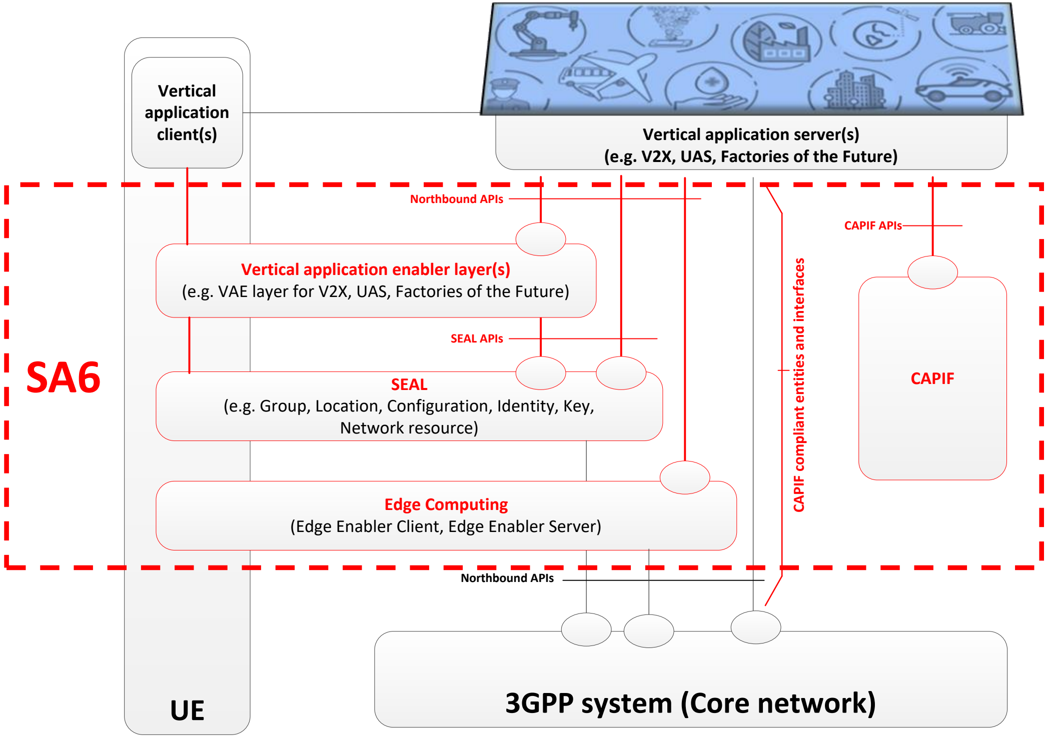


Application service provider
ASP service agreement
End user/UE
Edge computing service provider service agreement
Edge computing service provider
PLMN subscription arrangement
PLMN operator service agreement
PLMN operator

© 3GPP 2019

Leveraging SA6 for 5G Verticals

TS 23.222 [CAPIF] TS 23.434 [SEAL] TS 23.286 [V2XAPP] TR 23.758 [EDGEAPP] TR 23.755 [UASAPP] TR 23.745 [FFAPP]



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
SA6
SEAL
(e.g. Group, Location, Configuration, Identity, Key, Network resource)
CAPIF compliant entities and interfaces
CAPIF
Edge Computing
(Edge Enabler Client, Edge Enabler Server)
Northbound APIs
UE
3GPP system (Core network)

***CAPIF* - Common API Framework to aid 3rd party applications access to 3GPP functions**

***SEAL* - 5G Service Platform enabling common capabilities for quicker onboarding of new Verticals**

***Vertical Application Enablers* – Application support layer for vertical applications (V2X, UAS, FF)**

***Edge Computing* – Enables deployment of Edge Apps in compliance with 3GPP System for low latency and increased performance**

© 3GPP 2019

Overview: Rel-16 Work Items (Completed)

Work Item	WI Code
Enhancements for Common API Framework for 3GPP Northbound APIs	**eCAPIF**
Enhanced Mission Critical Push-to-talk architecture phase 2	**enh2MCPTT**
Enhancements to Functional architecture and information flows for Mission Critical Data	**eMCData2**
Enhanced mission critical system migration and interconnection	**eMCSMI**
Enhanced Mission Critical Communication Interworking with LMR Systems	**eMCCI**
MBMS APIs for Mission Critical Services	**MBMSAPI_MCS**
Application Layer support for V2X Services	**V2XAPP**
Service Enabler Architecture Layer for Verticals	**SEAL**
Application Architecture for the Mobile Communication System for Railways (MONASTERY) Phase 2	**MONASTERY2**

© 3GPP 2019

Overview: Rel-17 Work Items (Ongoing)

Work Item	WI Code	Initiated	SA#85 (09/19)	Target Completion
Enhancements to Application Architecture for the Mobile Communication System for Railways Phase 2	**eMONASTERY2**	06/2019	**70%**	12/2019
MC services support on IOPS mode of operation	**MCIOPS**	06/2019	**10%**	09/2020

© 3GPP 2019

Overview: Rel-17 Study Items (Ongoing)

Study Item	WI Code	Initiated	SA#85 09/2019	Target Completion
Study on Mission Critical Services support over 5G System	**FS_MCOver5GS**	06/2018	**40%**	(09/2020)
Study on location enhancements for mission critical services	**FS_enhMCLoc**	09/2018	**70%**	(03/2020)
Study on application layer support for Factories of the Future in 5G network	**FS_FFAPP**	12/2018	**20%**	(09/2020)
Study on application layer support for Unmanned Aerial System (UAS)	**FS_UASAPP**	12/2018	**25%**	(03/2020)
Study on Application Architecture for enabling Edge Applications	**FS_EDGEAPP**	03/2019	**70%**	(12/2019)
Study on Enhancements to application layer support for V2X services	**FS_eV2XAPP**	06/2019	**25%**	(03/2020)
Study on support of the 5GMSG Service	**FS_5GMARCH**	06/2019	**20%**	(06/2020)
Study on Mission Critical services over 5G multicast-broadcast system	**FS_MC5MBS**	09/2019	**20%**	(03/2020)

Summary

- 3GPP SA6 has established a mature set of MCX standards
  - Enhancements will continue!
- 3GPP SA6 is enabling support for vertical industries
  - Application Enabling Framework(s): CAPIF, SEAL, EDGEAPP
  - Vertical Applications Enablers: V2X, UAS, Factories, IoT/Messaging
- Participation from Verticals is essential: Please join us
  - Contribution-driven approach – Your voice will be heard!

© 3GPP 2019

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/

© 3GPP 2019