Deliverable 1.3

Overall 5G Convergent Control Plane Design

Editor:	Xueli An, Huawei Technoloiges
Authors	Task 1.2 Team: HUA, DTAG, ITAV, Telenor, BCOM, NEC, InterDigital
Deliverable nature:	(R) Document, Report
Dissemination level: (Confidentiality)	CO
Planned delivery date:	Draft March 2016, Final December 2016
Actual delivery date:	On Schedule
Suggested readers:	WP2 contributors, 3GPP SA representative
Version:	1.0
Total number of pages:	69
Keywords:	5G Control Plane Architecture

Abstract

To enable the integration of Verticals, to support efficiently a wide range of heterogeneous use cases and to allow the integration of different access technologies, 5G systems will require radical innovation in the core network architecture and technologies.

CONFIG aims at defining a *5G Convergent Core Network Control Plane*, meant to be the 5G cornerstone, enabling network slicing and allowing logical architecture tailoring according to performance and functional requirements of the supported services.

This deliverable provides key definitions, founding principles and overall high level design for 5G Convergent Core Control Plane.

Disclaimer

Impressum

Full project title: COntrol Networks in FIve G

Short project title: CONFIG

Number and title of work-package: WP1

Number and title of task: Task 1.2: 5G Control Plane System

Document title: Overall 5G Convergent Control Plane Design

Editor: Xueli An, Huawei Technologies

Task leader: Xueli An, Huawei Technologies

Copyright notice

Executive summary

This D.1.3 v.1.0 deliverable reports results and conclusions from the 1st phase of Task 1.2, which aimed at the **Overall 5G Convergent Control Plane Design**.

Starting from the Use Cases and Requirements analysis performed in Task 1.1, Task 1.2 **formalised a reference scenario** as well as key requirements for next generation networks, and **formulated the key design principles** for next generation core network architecture. Upon the key design principles, **5G Core Network Architecture Design Model** has been defined, and the **Overall High Level Design** has been completed.

Reference Scenario and Requirements

Technology trends [1]and market forecast[2] depict quite a clear scenario for telecommunication systems and services over the next decade. On one hand, together with smart phones, a wide variety of different devices will require connectivity (wearable devices, smart cars, electronic household appliances, industrial devices etc). Such devices will feature different/multiple access capabilities and they will be characterised by very different service requirements and data traffic models. On the other hand, the heterogeneity of the deployed access infrastructure (including new 3GPP and non 3GPP systems, as well as legacy 3G/4G networks, WiFi Hotspots etc) will represent both an opportunity and a challenge for next generation operators. Finally, the need to integrate communication services required by vertical industries completes the list of key requirements for next generation networks.

The requirements mosaic herein briefly summarised unambiguously highlights the **Core Network** will play a pivotal role in next generation networks. The needs to **integrate different access technologies** and to **tailor the *end to end* network architecture** according to functional and performance requirements of the supported services can be satisfied only via a Core Network conceived around a new set of design principles. In short, 5G system shall allow the definition of tailored end to end logical architectures integrating different access technologies, and to operate them independently one another.

Design Principles

Focusing on Control plane, CONFIG Task 1.2 formulated **three key design principles** upon which a 5G Core Network allowing the integration of different access technologies, the architecture customisation to meet different functional and performance requirements, and the integration of communication services required by vertical industries can be designed.

The design principles are (*details in section 2*):

1) **Architecture Modularisation**: 5G tailored end to end network architectures, including C-plane and D-plane, shall be defined upon a set of basic Building Blocks (BBs), including Access network and Core Network-related functions.
2) **Core Network Independence from Access**: 5G Core Network related basic BBs shall be defined minimising the dependency towards the supported Access Networks.
3) **Support of Independent logical Networks**: 5G networks shall enable the concept of Network Slicing. In this context, a network slice is an independent logical network, defined by the interconnection of a set of BBs, which can be independently instantiated and operated over a set of physical infrastructure, to support the communication service of a particular use case.

[1] Ericsson, “Ericsson Mobility Report, On the Pulse of the Networked Society”, June 2015.

[2] Cisco, “Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019”, White Paper.

5G Core Network Architecture Reference Model and High Level Design

Upon the key design principles, a 5G Core Network Architecture Reference Model (depicted in figure A) has been defined, and Overall High Level Design completed (*details in section 3*).

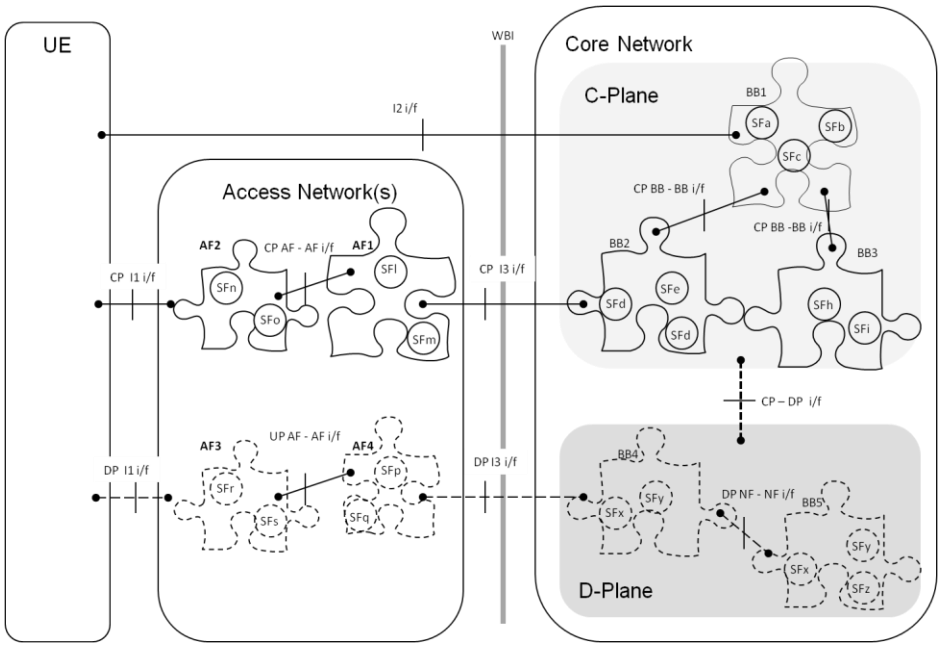

Figure A: Architecture Modularisation Reference Model

The Reference Model prescribes a strict separation between Control and Data planes, and defines the key architectural elements:

- **Basic Building Blocks**: a BB is an independent logical network function, made by elementary sub-functions, and accessible via interfaces or reference points. Different versions of a BB may be defined via a proper composition of elementary sub-functions. Different interconnections of different sets of BBs define different Logical Architectures fulfilling requirements of different use cases.
- **Inter Building Blocks Interfaces**: inter BB interfaces allow interconnection and information exchange among BBs (both for C-plane and D-plane)
- **Westbound Interfaces (WBI):** WBI allow interconnection and information exchange between Core Network and Access Networks, and between Core Network and UE.

The key set of BBs has been designed, and it includes (*details in section 3.2 – 3.6*):

- **Access Function (AF)**
- **Connectivity Management (CM)**
- **Security and AAA Management (SAM)**
- **Mobility Management (MM)**
- **Flow Management (FM)**

Sub-functions of each BB, required Inter BBs interfaces and WBI interfaces have also been identified (*details in section 4 and 5*).

The completion of the overall high level design will allow moving to the second phase of Task 1.2 where, upon the basic set of BBs, use case specific architectures and procedures for a few selected use cases will be designed in detail. Additionally, the architecture cornerstones set by Task 1.2 will trigger the design of Context Aware and Intelligent Connectivity solutions, focus of Task 1.4 and Task 2.2.

List of authors

Company	Author	Contribution
Huawei Technologies Düsseldorf GmbH	Riccardo Trivisonno, Riccardo Guerzoni, Xueli An	Sec 1, Sec 2.1, Sec 2.2, Sec 2.3, Sec 3.1, Sec 3.3, Sec 4, Sec 6, Sec 7
Deutsche Telekom AG Laboratories	Kay Haensge, Dirk von Hugo, Hans Einsiedler	Sec 2.2.4, 3.4, Sec 3.5, Sec 4, Sec 5, Sec 7
Instituto de Telecomunicações	Daniel Corujo	Sec 3.2
Telenor ASA	Kashif Mahmood	Sec 3.6
b<>com	Cao-Thanh Phan	Sec 3.4
NEC Europe Ltd.	Marco Liebsch	Sec 3.6
InterDigital Europe LTD	Dirk Trossen	Sec 3.6

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Definition
AS	Access Stratum
BB	Basic Building Block
CAPEX	Capital Expenditure
CM	Connectivity Management
FM	Flow Management
HSS	Home Subscriber Server
MEC	Mobile Edge Computing
MM	Mobility Management
MNO	Mobile Network Operator
NAS	Non Access Stratum
NFV	Network Function Virtualisation
OPEX	Operational Expenditure
SDN	Software Defined Network
VM	Virtual Machine
WAMCS	Wide Area Monitoring and Control Systems
CPE	Customer Premises Equipment
QoS	Quality of Service
QoE	Quality of Experience
SDN	Software Defined Networking
SAM	Security and AAA Management
VMNO	Virtual Mobile Network Operator
WBI	West Bound Interface

Definitions

Basic Building Block: BB is an independent logical network function, made by elementary sub-functions, and accessible via interfaces or reference points. Different versions of a BB may be defined, via a proper composition of elementary sub-functions.

Network Slice: A network slice is an independent logical network, defined by the interconnection of a set of basic building blocks, composing both C-plane and D-plane, and which can be independently instantiated and operated over a set of physical infrastructure, to support the communication service requirements of a particular or multiple use cases.

End to End Network Slice: a network slice spanning all the components of the communication system needed to provide devices with the requested communication service. E.g. for an eMBB network slice, providing a bearer communication service from the air interface (e.g. 4G Um interface) to the PDN anchor point (e.g. 4G SGi interface), “end to end” indicates the slice includes Radio Access Network components and Core Network components.

1 Introduction

1.1 Objective and Overview of the Deliverable

The objective of this deliverable is to provide:

- key definitions,
- design drivers,
- founding design principles and
- overall high level design

for a **5G Convergent Core Control Plane**.

The deliverable is structured as follows:

Section 2 provides an overview of the proposed 5G Convergent Network Architecture.

Section 2.1 highlights the **key high level requirements** making 4G systems unsuitable to support next generation services, while section 2.1 introduces three **key design principles** for next generation network stemming from such requirements:

- Network Slicing;
- Network Architecture Modularisation;
- Control plane toolbox;

Section 2.3 includes a **high level description of the proposed 5G Convergent Core Control Plane**, conceived around these principles. The concepts of Basic Building blocks, inter-building block interface and WestBound Interface are introduced in this section.

Section 3 describes the rationale behind the **proposed network architecture modularisation** and defines the key set of basic Building Blocks upon which different tailored C-plane architectures can be defined. Section 3 contains also a technical description of each Basic Building Block.

Section 4 defines Westbound Interfaces.

Section 5 lists and describes inter BBs interfaces.

Annex A lists the key C-plane procedures relevant to the design of next generation core network architecture.

Annex B collects references to relevant prior art.

2 5G Convergent Network Architecture: Overview

2.1 Key Design Drivers

Next generation telecommunication networks are expected to cope with diverse, sometimes conflicting, use cases. Discussions in various telecommunication fora during 2015 have identified a wide set of heterogeneous requirements for services and devices to be supported. The FP7 project METIS described a list of use cases [2] , deriving requirements on capacity, end to end latency, energy efficiency and reliability. The majority of those requirements cannot be efficiently fulfilled by 4G systems (e.g. LTE/SAE) and, more importantly, some challenging performance targets appear to be reasonable only for very limited scenarios. For instance, targeting very low end to end delay (in the order of 1-5ms) appears to be reasonable only considering a narrow set of communication scenarios and a limited population of devices admitted to such performance. Next generation network requirements received also the attention of standardization fora. A wide list of service and operational requirements with related market segments and verticals is available in the latest version of [3]. According to the document, the 5G system is expected to support a wide variety of use cases: ultra-reliable communications for mission critical services, Real Time Vehicle Control, Mobile Health Care, Virtual Presence, Tactile Internet (where low latency is defined by 1 ms), lifeline communications including location signalling during disasters and so on. **Supporting such an assorted set of use cases can be accomplished only by a flexible network, capable to adapt to achieve heterogeneous performance and functional targets.**

In addition, by 2020 a very high penetration of devices requiring connectivity will characterise densely populated urban areas. Devices (which will be either static, or nomadic, or mobile) will include Laptops, PCs, tablets, smart phones, augmented and virtual reality glasses, wearable devices and (electric) household appliances (such as e.g. building sensors for surveillance or refrigerators/washing machines). Such devices will embed multiple access technology chipsets, e.g. legacy HSPA, LTE, IEEE802.16x, IEEE802.11xx, IEEE802.15.4, plus all new forthcoming next generation access technologies. Connectivity will be the primary requirement for devices to provide the service(s) they are meant for. Services might be provided either by the same business (possibly virtual) actors providing connectivity, or by OTT entities. Each type of device will support a subset of all possible services, and some services will be supported by multiple types of devices. In parallel, by 2020, the deployment of physical access infrastructures, including cellular networks, WiFi hotspots, home xDSL connection, will have created a heterogeneous scenario where a variety of access technology shall provide ubiquitous broadband access. Mobile Network Operators (MNOs) or Virtual MNO (VMNOs) will deploy or will lease a mixture of physical access infrastructure to build their network and to serve efficiently their customers. MNOs and VMNOs will provide their customers with contracts guaranteeing mobile broadband connectivity according to a) devices capabilities and b) subscriber profile, integrating their physical / virtual access infrastructure**. In this expected scenario, supported by technology trends and telecom market analysis, next generation system shall enable MNOs and VMNOs to handle efficiently such heterogeneity of devices and deployed access networks, providing connectivity exploiting the most convenient access technology.**

Finally, **vertical business (automotive, smart cities, smart grids, Industrial Internet, eHealth, etc.) will also represent an attractive market segment** for next generation networks. New business actors (e.g. car makers, utilities providers, municipalities, health centres etc.) are expected to require communication services, with particular functional and performance requirements, to interconnect devices they will provide service to/via (e.g. vehicles, utility meters, environmental sensors, wearable devices for e-health etc.).

2.2 Key Design Principles

From design drivers briefly outlined in section 2.1, some **key features** for next generation networks can be identified:

- Architecture Flexibility;
- Heterogeneous Access Network Integration;
- Vertical Business Integration.

Architecture flexibility reflects the need to support efficiently heterogeneity of services and devices, generating wide set of functional and performance requirements, for which *any single architecture* cannot possibly be a solution. Hence, next generation networks shall not feature a single logical architecture but, rather it shall enable the instantiation of tailored end to end logical architectures targeting requirements of clusters of homogeneous use cases. Tailored architecture will include tailored Control Plane (C-Plane) and Data Plane (D-Plane).

Heterogeneous Access Network Integration results from the willingness of MNOs and VMNOs to exploit all deployed access infrastructure (wireless cellular, wireless non cellular, fixed etc.). For this reason, next generation network shall enable MNOs and VMNOs to handle efficiently the heterogeneity of devices and access networks deployed, providing connectivity exploiting the most convenient access technology. The way MNOs/VMNOs will provide connectivity to users shall depend on a number of factors, including:

- The contract agreement with the users;
- The device type and service/application type;
- User Context information (e.g. location, mobility profile etc.);
- MNO/VMNO Network load;
- MNO/VMNO Resource availability and related cost.

It is relevant to highlight that, unlike 4G system (i.e. LTE/SAE), where *INTERWORKING* of different Radio Access Networks is achieved via the definition of interfaces and procedures among 3GPP and non-3GPP Core Networks, next generation system shall aim at achieving heterogeneous cellular and non cellular access network *INTEGRATION, rather than* INTERWORKING: 5G Core Network shall be able to support directly different access networks, regardless of legacy core networks previously developed.

The ability ***to integrate Vertical Business*** is another relevant feature for next generation network. It will enable operators (MNO/VMNO) to evolve, incrementally, their networks as soon as new additional requirements will emerge from new services vertical industries will have to provide. Integration of Verticals also relates to the ability to operate, in parallel, different isolated logical networks, instantiated within a common set of physical infrastructure.

Combing the need for these three key features with the current development of NFV, SDN, Cloud Computing and MEC technologies, led to the definition ***of founding design principles*** for 5G:

- Network Architecture Modularisation;
- Convergent Core Network;
- Network Slicing;
- 5G C-plane toolbox.

5G Design Principles are described in the following subsections.

2.2.1 Network Functional Decomposition: Access/Network Function

For enabling the design of tailored logical architectures, including C-plane and D-plane, and fulfilling requirements of clusters of homogeneous use cases, **a set of Basic Building Blocks (BB) will be**

defined. *A BB is an independent logical function, made by elementary sub-functions, and accessible via BB interfaces or reference points.* Different customized BBs may be defined, via a proper composition of elementary sub-functions.

Logical functions can be classified in *Access Network* functions and *Core Network* functions.

Also, logical functions may relate to C-Plane or to D-Plane.

The principle behind this design choice is to decompose the logical network architecture in basic modules of the proper granularity (the BBs), by interconnection of which different tailored C-plane and D-plane architectures can be defined. BBs can be customised (e.g. including/not including certain sub-functions) and also dynamically instantiated in the cloud infrastructure according to network operation or service requirements.

It is relevant to observe the concept of tailoring C/D-plane is twofold. From one side, tailoring means the adaption of the C-plane procedures to performance requirements of applications and devices. For instance, procedures may be simplified for use cases where minimising signalling can be a relevant design goal, to reduce the risk of control plane congestion. From another side, it regards the selection and the implementation of the set of functional blocks included in the C/D-plane: different BBs can build C/D planes of different slices, and as far as concerning their implementation, BBs can be either centralized or distributed, depending on service functional and performance requirements.

Design Principle I: 5G tailored end to end network architectures, including C-plane and D-plane, shall be defined upon a set of basic Building Blocks including Access network and Core Network-related functions.

2.2.2 5G Convergent Core Network

In the process of decomposing the logical network architecture in basic modules, the distinction between BBs relating to *Access Network* and *Core Network* will emerge.

Based on a rational distinction between Access Network and Core Network BBs, the dependency of 5G Core Network on different Access Networks might be minimised, this leading to the definition of a Convergent Core.

Identifying Core Network related BBs will have to consider Access Networks which will not only include 5G RAN: a convergent core shall be able to provide connectivity via a multitude of access networks and technologies, including legacy/future cellular/non cellular radio/wired access.

The definition of Core Network-related BBs shall allow the definition of tailored and access independent C/D-plane architectures, compatible with different Access Network-related BBs.

Design Principle II: 5G Core Network related basic Building Blocks shall be defined minimising the dependency towards Access Network characteristics.

2.2.3 Network Slicing

The definition of tailored logical network architecture, which may be independently instantiated and operated on common physical infrastructure, leads to the concept of network slicing.

A network slice is an independent logical network, defined by the interconnection of a subset of basic building blocks, composing both C-plane and D-plane, and which can be independently instantiated and operated over a set of physical infrastructure elements, to support the

communication service requirements of a particular or multiple use cases.

As use case requirements are defined end to end, regardless of any design consideration distinguishing between segments of the communication system, the network slice is defined across the whole communication system, hence including both Access and Core networks. Slicing may also involve resources of the last hop connection to the device, including spectrum, radio resources etc.

The implementation of the concept of network slice requires tackling three key issues:

- Slice(s) design;
- Slice(s) instantiation;
- Slice(s) operation.

Designing a slice requires the definition of C-plane and D-plane architecture, procedures, and protocols upon the basic set of Access and Core Networks-related BBs.

Instantiating a slice deals with mechanisms for its implementation and deployment over the available physical infrastructure.

Finally, *operating* slices requires mechanisms for configuration, management and monitoring them.

Design Principle III: 5G networks shall enable the concept of Network Slice.

2.2.4 5G C-plane Toolbox: Access/Network Function

As outlined in [28], a 5G slice is defined as composition of a set of 5G network functions in core and access domain combined together such that the specific demands of a use case or business model are fulfilled in an efficient way. While some functions have to be present in any slice, not all slices contain the same functions, and a function (such as e.g. Mobility Management) may be essential for one slice (e.g. Mobile Broadband) but missing in some other slices (e.g. Fixed Residential Access or IoT).

The key concept of creating a toolbox of modular network functions and protocols allows designing and implementing a specific network slice which is based on the flexibility of SDN and NFV concepts. Hence, it offers the possibility to assemble and orchestrate software instantiations which define the virtual network functions. These functions are based on a collection of available software components and building blocks allowing for network architecture construction on the fly and for various time periods. The network architectures will be constructed based on the requirements of the specific use case or application area.

From the point of an operator and per slice, two kinds of toolboxes will exist. The operator internal toolbox – operator repository –, which contains the standardised network functions and protocols of the operator. The other toolbox is external and is an application or use case repository, which contains use case specific network functions with standardised interfaces. The network services will be offered by the use case owner and can be brought into the orchestration of the 5G C-plane/core network.

Based on the set of use cases from application areas described in Del. 1.2 [29], the required basic building blocks for a specific network slice are chosen from the toolbox as denoted in Figure 1 and Figure 2. The idea of a toolbox with different very generic building blocks and clear interfaces to support an easy handling and orchestration of the infrastructure set-up was already described in [30]. The resulting flexible and configurable 5G C-plane will make it possible to create connectivity services for a multitude of use cases with the intent of supporting both already existing and yet unknown future use cases.

Note that technology aspects of the data plane (D-plane) are not in scope of this architecture, as we expect that D-plane improvements will be dominated by hardware technology developments (seamlessly included in network by SDN concepts).

The content of the toolbox in terms of basic building blocks will be specified throughout this Deliverable, especially in Section 3. The detailed definition of the tools will be found in Section 3.1 whereas the sections following thereupon describe details of each basic building block.

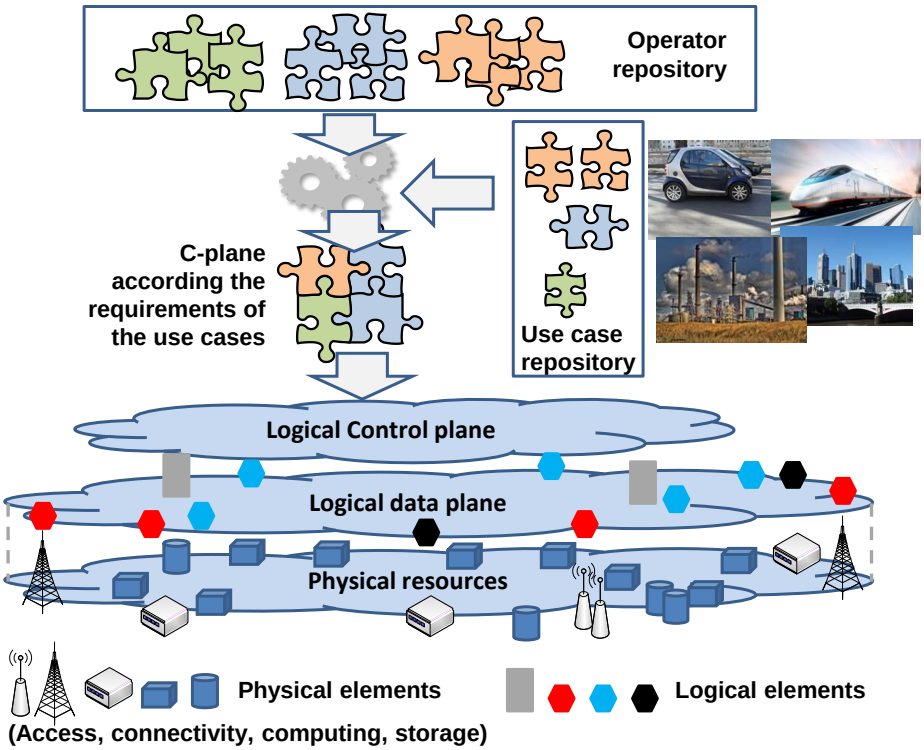

Figure 1: 5G Network function toolboxes (repositories)

2.3 5G C-plane High Level Design

Upon design drivers and principles analysed in Sections 2.1 and 2.2, the high level design for 5G Convergent Core Network Control plane architecture is presented in this subsection. The reference framework is illustrated in Figure 1. The picture highlights the 5G C-plane, the key basic building blocks and related interfaces (I/F). The scope of 5G C-plane high level design is limited to the core network C-plane architecture, and does not include the specification of northbound (i.e. towards 5G Communication Services) and southbound (towards access and network infrastructure controllers) interfaces, which are anyway defined for sake of completeness.

The interface between 5G C-Plane and 5G Communication Services and application developers (I/F (3)) allows the transfer of use case specific information bi-directionally to the control platform, which will act upon all aspects of service invocation in the C-plane. Use case specific information includes services functional and performance requirements, devices deployment information, users' traffic patterns, monitoring information, and mobility profiles etc. Additionally, via I/F (3), C-plane specific information is provided to external users, service providers and customers. Via I/F (3'), application specific network functions from the 3rd party customers could be used.

5G NF I/F (1) allows interaction between BBs. In particular, 5G NF I/F (1) between Access Network related and Core Network related BBs is the key interface enabling access convergence, as it allows communication and interworking between 5G core network and access specific functions. This I/F is also referred as Westbound Interface (WBI).

Network physical infrastructures are controlled by the Network Infrastructure Controller, connected to Core Network related BBs via access independent I/F (2). Access network physical infrastructures are controlled by access specific BBs through the Access Controller to which they are connected via Access Specific NF Controller I/F (2').

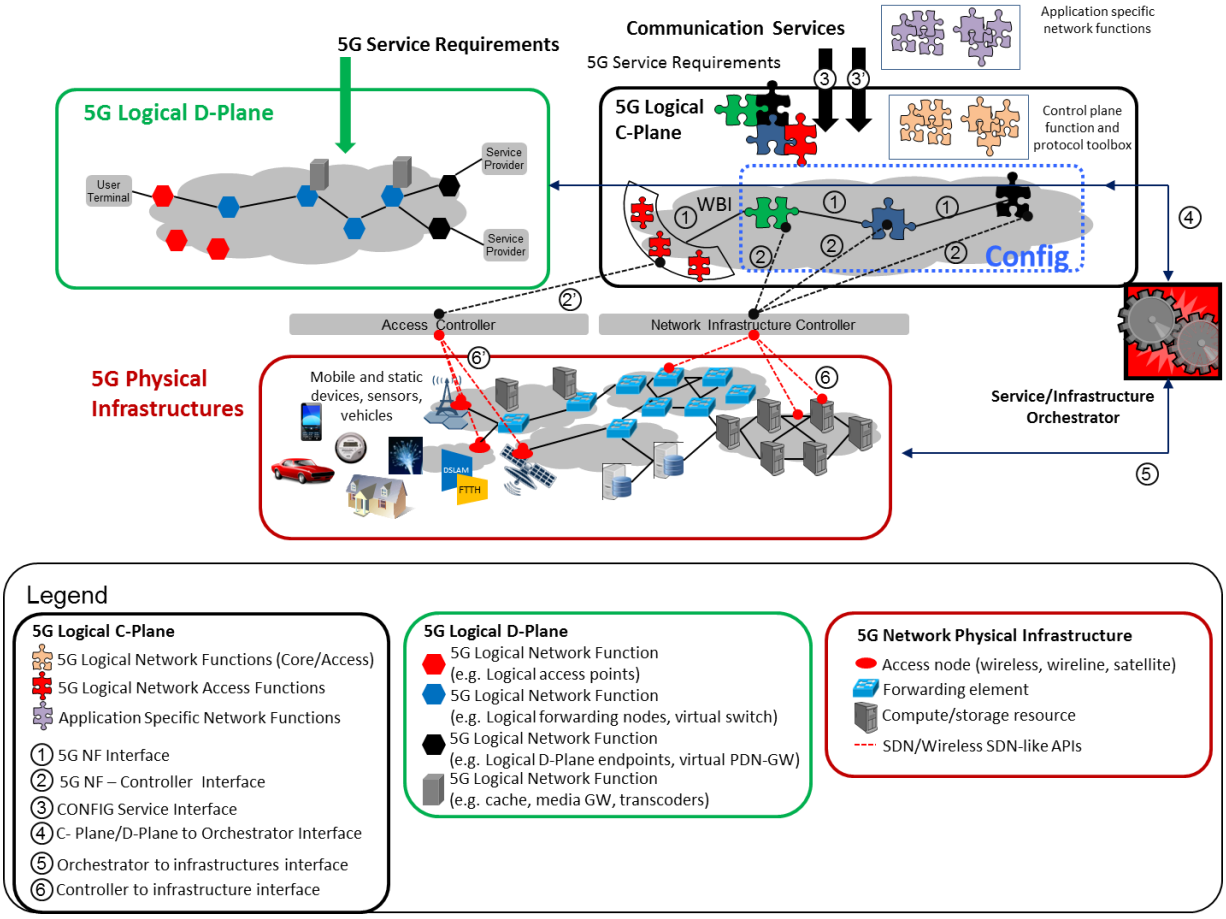

Figure 2: 5G Network Reference Framework.

The right side of the picture shows also the interaction between C-Plane and Service/Infrastructure Orchestration entities. The Service Orchestration module is in charge of defining instantiations of C-plane, according to service and device requirements received from I/F (4), and to implement them on the physical infrastructure via the related I/F (5). Similarly, the Infrastructure Orchestration/SDN Configuration module orchestrates and defines resources configuration for D-plane based on the requirements received from I/F (4), which are instantiated via the related I/F (5).

In this reference framework, the C-plane design needs to solve three distinct problems:

- Definition of the Basic Building Blocks;
- Definition of Inter Building Blocks Interfaces;
- Definition of Interfaces between Access Network-related and Core Network-related BBs.

2.3.1 Basic Building Blocks

The first design issue to address is defining a suitable set of BBs.

The definition of the set of BBs requires considering:

- The choice of a proper *granularity* for BBs, which is influenced by the trade off between the need of flexibility (to compose tailored architectures) and the complexity relating to inter-BBs interfacing;

- The definition of separate sets of Access Network-related BBs and Core Network-related (i.e. access independent) BBs, to ensure the possibility of designing access independent core networks.

The design of a set of BBs, schematically represented in Figure 3, is addressed in Section 3.

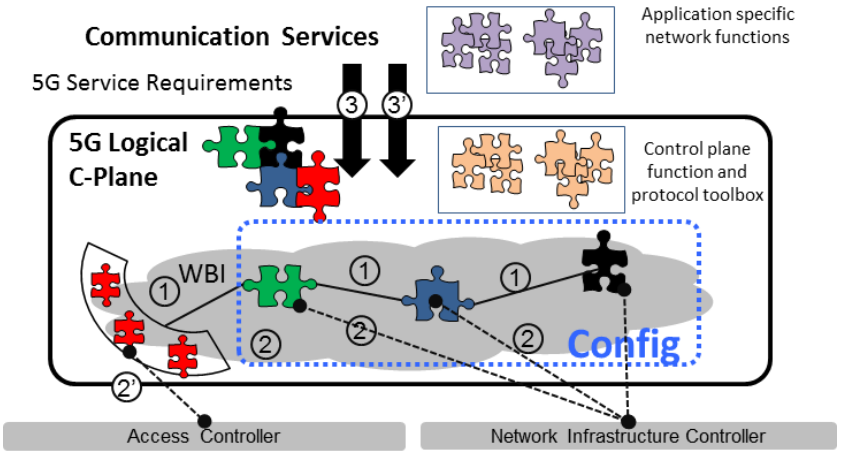

Figure 3: BBs, Inter BBs interfaces, BBs to Controller Interfaces

2.3.2 Inter Building Blocks Interfaces

The second design issue to address is defining the required interfaces among BBs.

Inter BBs interfaces are defined in sub Section 3.2 - 3.6, and summarised in Section 5.

2.3.3 West Bound Interfaces

The third design issue to address is defining the interfaces between Core Network-related BBs and Access network related BBs as well as device. This set of interfaces is defined as West Bound Interfaces.

Westbound interfaces are defined in Section 4.

3 5G Basic Building Blocks

3.1 5G Basic Building Blocks Definition

The key issue to address moving forward towards **network architecture modularisation** is the definition of **a set of Basic Building blocks** which allow the design of tailored slice architectures, fulfilling functional and performance requirements of clusters of homogeneous use cases.

A Basic Building Block (BB) is an independent logical entity, dedicated to perform a set of network functions and accessible via interfaces.

BBs can be classified in **Access Network** related and **Core Network** related.

To achieve the design of end to end slice architectures capable of integrating and steering heterogeneous access networks, **access independent Core Network BBs** need to be defined.

Defining the set of Core Network BBs requires first of all to define their granularity. To this end, the trade off between flexibility and complexity needs to be considered.

A huge number of elementary BBs would provide the highest flexibility in slice architectures definition, but the complexity would also pose hard feasibility challenges. Complexity would affect:

- Control/data plane procedures (several BBs would be involved in message exchanges);
- Inter-BBs interface definition (interfaces to be defined for each interacting pair of BBs);
- Distribution and maintenance of network/device information across several BBs.

On the other hand, too few BBs wouldn't allow significantly differentiation of the architecture of different end to end slices.

Additionally, the definition of BBs granularity needs also to consider business related factors. BBs, instantiated as software elements within SDN/NFV based could infrastructure, will replace in next generation networks the 4G physical/virtual network elements. Also, Verticals, as business actors, might develop proprietary BBs to customise slices to provide ad-hoc services.

The balance between these conflicting issues can be achieved defining BBs grouping homogeneous network functional areas (to avoid a too fine granularity) and to further design each BB as the composition of elementary sub-functions, mapping with "atomic network function".

A draft set of BBs has been achieved analysing the full list of network functions included in 4G networks and adding additional ones which are expected to be 5G distinguishing features.

Table 1 summarises the 4G network function analysis and the grouping to define BBs. The table is derived from an in depth analysis of 3GPP specifications ([4], [5], [6]) and it includes all main AS/NAS functions. The 1st column identifies the function class; the 2nd column identifies the 4G function name, 3rd column indicates if the function is access dependent. Some functions clearly access dependent in 4G system must be made independent in order to achieve a convergent core network, capable of integrating non 3GPP accesses. The 3rd column indicates "YES" for 4G access dependent functions, "NO" for 4G access independent functions, "NO (YES)" for 4G access dependent functions that have to be turned access independent in 5G.," Finally, the 4th column defines the BB to which the function will be associated. Note that some functions are considered out of Core Network scope, as they relate to the network management domain.

From the analysis summarised in Table 1, the following set of BBs has been defined:

- Connectivity Management (CM);
- Mobility Management (MM);
- Security and AAA Management (SAM);
- Flow management (FM)

- Access Function (AF).

Each BB is discussed in details in the following subsections.

Table 1: Network functions grouping into BBs

AS/NAS Function Class	Function	Access Dependent	BB
Network Access Control	Network/Access Network Selection	YES	AF
	Authentication and Authorization	NO	SAM
	Admission Control	NO (YES)	CM+AF
	Policy and Charging	NO	SAM
Packet Routing and Transfer	Packet Routing	NO	FM
Mobility Management	User Reachability	NO	MM
	Tracking Area Management	NO (YES)	MM
	Paging	NO (YES)	MM
	Handover	NO (YES)	MM
Security	AS Security Control	NO (YES)	SAM
Radio Resource and Resource Management	Radio Connection management	NO (YES)	CM , AF
	Forwarding Path management	NO	FM
Network Management	Control Plane overload control	NO	Out of scope
	Data Plane overload control	NO	Out of scope
	5G C-plane instantiation	NO	Out of scope
	5G C-plane maintenance	NO	Out of scope
	Load balancer	NO	FM
Addressing Functions	DNS address resolution	NO	CM
	Address Allocation	NO	CM
Proximity Service	Proximity Discovery	NO (YES)	MM
	Direct Communication	NO (YES)	CM
Relaying	Relaying	NO (YES)	CM+MM
Mutual Authentication	Mutual Authentication	NO	SAM
5G Specific	Slice Management	--	CM
5G Specific	Inter slice mobility	--	CM
5G Specific	Context Awareness Optimisation	--	CM

3.2 Access Function Block (AF)

The provisioning of connectivity and packet transport services in a converged environment will require interaction with different access technologies, each with its own means of operation and specificities. In order to support novel degrees of flexibility and fully incorporate the dynamic specification and orchestration of the underlying network connectivity services, novel ways are needed to interwork the procedures of the core network and access specific functions.

Even just considering specific network functions, such as network attachment and mobility, the different access technologies provide ample differences in regards to their utilisation, in different scenarios. Further complexity is manifested, even within the same standardisation body, when an inter-technology interaction is attempted (as is the case of offloading mobile traffic towards WLAN by the 3GPP [7], which become particularly challenging when considering the provisioning of IP mobility support between different access technologies [8]). As a consequence, despite existing standardisation efforts, seamless inter-technology connectivity with mobility support is yet to reach a satisfactory deployment capability in current networks. Different aspects contribute to this, such as inadequacy of deploying existing mobile architecture policy and charging control over non-mobile instantiations. Furthermore, with the enhancement of standards to incorporate new mechanisms (i.e., Mobile Edge Computing), new dependencies are created over the base mobile architecture which hinders reaching a mature inter-technology approach.

In respect to this, CONFIG, with its objective of allowing the connectivity establishment to be much more dynamic, while operating under a converged environment, must rely on a set of more flexible mechanisms to convey converged control plane assessments over the different access technologies. As such, a fundamental part of the set of CONFIG functions is the Access Function. Despite that, within the project, the actual realization of the connectivity provisioning process for the access networks is out of scope, the function will contribute with the definition of interfacing components towards access-specific control planes, thus assisting the other CONFIG functions by providing them with a single means for that purpose.

A fundamental guideline for the elaboration of this entity, is the consideration of interaction requirements by the other CONFIG functions, in regards to access network control, taking into consideration important aspects, such as abstracting connectivity procedures (i.e., access network point of attachment discovery, resources evaluation, registration, authorization and others). Current standardisation efforts, such as IEEE802.1cf [9], have started to define reference models that make use of technologies that compose a fundamental role in the upcoming 5G architecture, such as *Software Defined Networking*, which support the abstraction and functional decomposition of procedures such as:

- Setup of interfaces and nodes
- Detection of node attachment
- Path establishment, maintenance, relocation and teardown
- Coordination and Information of access aspects
- Event handling between the Core and Access layers
- Statistics gathering

The next subsections highlight important operational points of this function, in regards to its interaction with the other CONFIG functional entities.

3.2.1 Function Tasks

3.2.1.1 Providing connectivity on access network (out of scope)

Despite that the objective is not to actually provide the connectivity for the access network (that will be explored in another 5G project, namely 5G NORMA [10], the AF must be perceived as the entity

that will provide the necessary interfaces towards access network control.

3.2.1.2 Terminating Westbound interface

The interaction between the Control plane and the Access network control entities (amongst other interactions) will be instantiated via the Westbound interface. Particularly, it is expected that the AF features the means for this interface to provide support for network attachment and mobility, as well as access node configuration. It is expected that the different access networks involved will provide specific control interfaces themselves, abstracted by a single interface towards the control plane side.

3.2.1.3 Support connectivity operations

The AF should also manifest itself as the converging point for access network-initiated mechanisms, such as initial access, transition or re-entry of end devices into the access network, towards the control plane.

3.2.2 Related C-Plane Procedures

3.2.2.1 Setup of interfaces and nodes

The AF should assist towards the configuration of the different parameters involved in the configuration of nodes (and their interfaces) into the data path, or of any control link towards such devices. Parameters can vary according to the type of access interface and node, ranging from identifiers, addresses, supported protocols or connectivity timers. Special considerations should be done according to *short-time-scale* and *long-time-scale* configurations, as these can have different specificities that may impact control plane connectivity provisioning.

3.2.2.2 Detection of node attachment

It can be assumed that the user terminal will be unaware that it is connecting to a CONFIG-enabled network and, as such, it is necessary for the AF to assist in abstracting the detection of the attachment of new terminals. Different technologies possess different mechanisms towards this detection, so some form of mapping or generalization must be provided towards the control plane.

3.2.2.3 Path establishment/teardown/maintenance/relocation

The concretization of connection establishment procedures at, for example, Layer 3 need to be complemented with according L2 procedures, in the eventuality of a mobility, connectivity or re-connectivity action. Independently of the slice deployment, there is the need to actually notify access network controllers about the existence of new flow(s), including potential requirements such as capacity, delay and jitter. Such information can be leveraged to establish a path into the access network data path elements, and enforce the control plane connectivity establishment decisions.

Complementary mechanisms might be necessary such as the ability to compute optimal paths, packet/frame matching and modification according to control-plane policies, application of forwarding rules, as well as actions to be executed over the packets themselves.

Reciprocal actions, such as path teardown, require complementary actions such as freeing up resources at the access network that are no longer necessary. This can be assisted by the availability of monitoring mechanisms or flow events. These can trigger decision entities at the control plane, which can decide on the actions to be taken at access network level, via AF support.

Such aspects are valid not only for data paths, but also for control paths that traverse into the access network. Typically, control path sessions outlive data path sessions and, thus, maintenance mechanisms are also needed. Therefore, record mechanisms with details about current paths might be required.

Finally, considering mobile environments or even due to traffic engineering aspects, data paths (as well as control paths) can have the need for being relocated. In this way, it is necessary to execute an establishment of the same path in the handover candidate point of attachment, transfer context therein, and teardown the previous path. The resulting outcomes of these actions require the provision of feedback towards the control plane.

3.2.2.4 Event handling

One very powerful, if not absolutely necessary aspect of flexible network operation is the shaping of its operation in strict regard to the dynamics of the current network conditions, and how they are affecting the user equipment. As the most common utilization case is mobile scenarios, many physical factors impact the quality of the wireless link reception, along with the increasing number of simultaneously connected users competing for medium resources. In this way, it is important that the network decision entities at the control plane have readily information on how the network is perceived by the user equipment, not only in terms of the current link, but also to be informed of which points of attachment are within range of the user (contemplating potential handover candidates). Such information cannot be provided by monolithic OSS/BSS and traditional monitoring systems, whose information base can be measured in a resolution of hours, if not days. The future converged 5G network architecture needs to have in place mechanisms which allow decision entities to be readily notified about these dynamic changing conditions. Moreover, it is necessary that such information can be provided in a generic form, independently of the underlying access technology. As such, events, which can be considered small informational signalling that is sent when specific network behaviours, are generated and sent out to interested entities, able to trigger appropriate reactions. Supportive event management mechanisms, such as allowing entities to register and define event notification configuration aspects at the source, are also needed. Also, such events can also be generated by network entities, such as an Access Point indicating to the control plane that it its currently experienced load has passed a previously configured threshold.

3.2.2.5 Statistics Gathering

Another important aspect that requires access network abstraction is the ability to provide statistics about the access current conditions. Such statistics prove invaluable for the maintenance and optimization of network operation. On one hand, each access technology is capable of generating specific statistics, which might not be replicable by other technologies. On the other hand, it is necessary to devise a common and generic definition of statistics, which is able to be perceived by the control plane, independently of the affected technology. Potentially, such generic approach can also be complemented by a mapping mechanism, which can further support decision entities in regards to the specificities of different access technologies.

3.2.3 Required Information

As an abstraction interface entity, the AF should not require information, or even store any, by itself. It should merely operate as a vehicle between information producers and consumers. However, the AF should feature some aspect of self-operation support information to assist and maintain state about its mechanisms. For example, storing the identification of entities that have registered the reception of events from sources that fall within the jurisdiction of that AF. Another example, can also be the storage of which access network entities are served by that AF, indicating different aspects such as supported events, its identifiers and other characteristics. Finally, and targeting more operational optimization, the AF can also act as a cache for information about access network elements, avoiding the need to constantly query the intended access network entity, thus saving on signalling, or even preventing the unnecessary wake-up of access entities, in case such technologies support more aggressive energy conservation measures.

Overall, the AF, as an intermediate between different kinds of access network information, can

potential have access to (as well as store) different kinds of information, which can include (but are not limited to):

- Subscription (for events) information, identifying the requested events, the involved entity and the requester entity.
- Access policies to information and control aspects of access network entities (i.e., indicating which kind of actions can be executed by which entities)
- Access network specific details, such as :
  - Link layer capabilities : MTU, encryption capabilities and others
  - Link layer performance: throughput up/down, delay, jitter, residual error rates (these can be indicated either as a list of parameters or by records representing different service classes).
- Access router : indication of which access router(s) that specific access network is connected to, along with information about :
  - Network layer Capability : IP address, size of IP network, IP version, IP configuration support and service discovery capabilities
  - Network interface performance : supported service classes, throughput up/down, delay, jitter
  - Offered application services: indication about application services reachable by the access router interfaces.

3.2.4 Interfaces to Other BBs

3.2.4.1 AF - CM

Provisioning of access related signalling messages and parameters by the AF to the CM, as well as coordination of the usage of common resources, with the AF receiving configuration and optimization commands from the CM.

3.2.4.2 AF - MM

The AF should be able to provide access related signalling messages and parameters, in an abstract way, made available by access network specific controllers. Such information should include attachment information about the device in the network, or even handover-related signalling from the access network entities. Such aspects need to be coordinated as well with the remainder of the control plane, since involved resources can be sliced/virtualized.

3.2.4.2.1 AF - SAM

The AF should be able to assist the SAM in access connectivity procedures, by providing access related signalling messages and parameters, in an abstract way. This interaction, made available by access network specific controllers, should encompass subscription services and involved procedures, such as AAA, roaming permissions and overall network connection policies. Such aspects need to be coordinated as well with the remainder of the control plane, since involved resources can be sliced/virtualized.

3.2.4.3 AF - FM

The AF should be able to able to provide access related signalling messages and parameters, in an abstract way, when required.

3.2.5 Required sub-functions

3.2.5.1 Control entity

Entity acting as the termination of SDN signalling, considering the potential existence of access network specific controller interfaces. The need for the AF to act as an intermediate for this signalling (and this needing to terminate it), can be required when there is need for abstracting or translating specific access technology procedures into generalized signalling to be sent towards the control plane (even though that the architecture should also support the possibility of allowing direct interaction between access network elements and control plane elements, when such situations are beneficial).

3.2.5.2 Event registry management

This sub-function allows the AF to maintain state about event capabilities of the access network, and interested entities about specific events (and their requesting configuration).

3.2.5.3 Subscription management

This sub-function contains elements identifying permissions for identifying which control plane entities have access/modification rights for access network configuration and modification.

3.2.5.4 Path record

In mobility-related scenarios, this entity has a record of the latest path (or next hop) towards interfacing entities (i.e., if a controlling entity has been shifted into another network slice, this is updated here, in case said entity had previously received to receive events about a particular element of the access network under jurisdiction of this AF).

3.3 Connectivity Management Block (CM)

Connectivity Management (CM) is the main engine in the C-plane to handle "connectivity" related procedures. The connectivity considered in the scope can refer to physical connectivity (for instance radio links allocated in the radio access network, and/or the flows allocated in the core network) as well as logical connectivity (e.g. bearers). The logical connectivity includes C-plane flows as well as D-plane flows.

A device may maintain single or multiple-connectivity within one or more than one access networks and via one or multiple flows within the core simultaneously. This section and related sub-sections explain the design considerations for CM.

The justification for CM being an independent BB in CONFIG is because it provides the fundamental C-plane service for 5G devices, it is a compulsory and major BB for all type of 5G slices.

In the following subsections, the detailed function tasks, related C-plane procedures, required information, interfaces, as well as sub-functions of CM are introduced.

3.3.1 Function Tasks

3.3.1.1 Device convergent state machine and corresponding information management

CM is the entity that is used to maintain device convergent state machine and its corresponding information. Such state machine may cover possible device state defined in variant access networks. While, the definition of state may be different from access network to access network. In general, a device could be in attached state (authorized by the network) or unattached state (not authorized by the network). For instance, in cellular network, a device can be in active state (with radio resource

allocated) or idle state (without radio resource allocation). A finite device states need to be defined which can be used to describe the device's status and behaviour in the network.

3.3.1.2 Device identifier management

CM is responsible to dynamically allocate a routable instance (e.g. IP address) for a device to access the network to demand or to participate in a service session. A device may require more than one more than one such instances for different access networks.

3.3.1.3 Device configuration

CM can discover a device's capability and connectivity relevant parameters. For instance, a device can be a single-slice capable (e.g. sensors for IoT or MTC) or multi-slice capable (e.g. smartphone, tablet). A device can also single-AN capable (e.g. with single access capability like LTE) or multiple AN capable (e.g. with multiple access interfaces like WiFi, LTE, etc.). CM can suggest certain configurations for devices (e.g. using WiFi other than LTE) for optimization or offloading purpose.

3.3.1.4 Access network configuration

CM handles the connectivity related procedures, hence CM has a global view of device and access network resource related usage information. Hence, it can provide AF building block related configuration parameters. One example could be that CM distributes the address of DNS servers to the access networks. In 4G scope, such configuration information could be the RAT/Frequency Selection Priority (RFSP) Index sent from MME to the eNBs. Other examples could be, device connectivity information is maintained in CM, which can be used to understand network congestion situation (C-plane and D-plane load).

Therefore, CM can inform AF to adjust provided data rate for devices or suggest device to use other access networks for traffic offloading. CM can also provide device-specific configuration parameters, e.g. suggesting the RAN settings for devices, e.g. for optimization purpose.

3.3.1.5 Slice management

CM is the key entity for the system to enable network slicing concept. CM is responsible to manage slices related procedures and activates, for instance slice attach, slice handover/switching, slice de-attach, etc. Dynamic provisioning to devices and access networks of slice-related configuration parameters.

3.3.1.6 Context awareness engine

Context is defined as the information that can be used to characterize the situation of an entity [11]. Example context could be available resources (e.g., access network, core network, as well as device characteristics), device type, user preferences (e.g. low budget, high throughput, etc.), and user environment (a location as well as the semantic meaning of the location) (e.g. shopping mall, train station, home, etc.). CM is responsible to perform context information mining and maintenance role in the entire C-plane. This sub-function has the potential to become an independent Building Block.

3.3.1.7 Manage the D-plane Anchor Endpoints

One of the primary tasks of the CM is to handle all tasks related to the management of the D-Plane anchor points. This involves selection and configuration of anchor endpoints (as indicated by the blue circles in Figure 4) to enable connectivity. How to establish connectivity in-between the endpoints is the task of FM, which will be introduced in Section 3.6, or it may rely on default rules in the D-Plane nodes in between these endpoints. In order to perform the above mentioned function, CM needs to have the abstraction view of the anchor endpoints within the transport network.

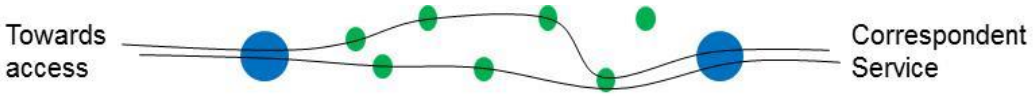

Figure 4: The role of CM is to manage only the blue nodes

3.3.1.8 Enforce and manage QoS policies on D-plane Anchor Endpoints

This involves resource reservation for critical flows based on QoS profiles. CM may contact AF to obtain information about the access network for QoS enforcement.

3.3.1.9 Legacy NAS translation

This task is optional, while it aims to provide system backward compatibility to the legacy networks like 4G LTE.

3.3.2 Related C-Plane Procedures

3.3.2.1 Device Attachment

The device attach procedure is the very first procedure performed between device and CM, which is used to register the device with the network in order to receive services that require registration. The attach procedure may trigger network to allocate resource for the device to receive services from the network, e.g. allocate IP address, setup flows, etc.

The attach procedure is slice specific. A device may attach to one or more than one slices.

3.3.2.2 Device De-attachment

The device detach procedure allows a device to inform the network that it does not need to access to the network any more, or the network to inform the device it does not have access to the network any more.

The de-attach procedure is slice specific, which means, a device may de-attach from one slice, but still attach to the other slice at the same time.

3.3.2.3 Device Authentication and Authorisation

This procedure performs mutual credential check to allow a device to access and receive services from a network. CM sends device related information for SAM for authentication. In Config scope, authentication and authorisation procedure is slice based. Different schemes can be used for this purpose. First, one device authentication and authorisation procedure may authenticate multiple slices that can be used by a device. Second scheme, one device authentication and authorisation procedure is required for each slice.

3.3.2.4 Device Triggered Service Request

This procedure is performed by a device, which has been attached with the network and requires to allocate resources from the network for the device, for instance, allocate radio resource at the air interface, setup flow path at the core network, etc.

3.3.2.5 Network Triggered Service Request

This procedure is performed when there is downlink data to be sent from the network to a device that has been registered with the network and it requires to allocate resources for the device.

3.3.2.6 Device Address Allocation

A device may perform this procedure to obtain at least one addresses from the core network. The

CM is responsible to allocate one or more addresses to the device.

3.3.2.7 Inter AT Handover

Vertical handover is used to support device changes from one access network to another access network. If the access networks belong to the same slice, then vertical handover only triggers D-plane update without C-plane changes. If the access networks are in different slices, such vertical handover triggers slice switching, which result into C-plane and D-plane changes.

3.3.2.8 Inter Slice Handover

This procedure is used to support a device to switch from one slice to another slice. This procedure can be triggered by CM or device.

CM can use its global view and/or context information to inform a device to switch from one slice to another slice. For instance, a user drives his car on highway, his mobile phone may connect to a slice with high mobility support. After he parks the car in his garage, his phone may switch to a slice with low/no mobility support.

Another example is, if a slice is congested, the CM may enforce certain devices (e.g. with low priority settings) to another slice with low performance profile but sufficient capacity.

As indicated by the examples mentioned above, slice handover/switching is not necessary a procedure triggered by mobility related events, but mobility events may result into slice switching.

3.3.2.9 Statistic/Context Information Retrieval

CM can obtain access network information from AF and transport network information from FM or the network controller of D-plane via SBI, which is further discussed in Section 3.3.4.6 and FM Building Block in Section 3.6. Such information may be further mined by CM to generated device and network context information which can be used by other Building Blocks for instance for optimization purpose.

3.3.3 Required Information

CM is the place to gather device and network related information.

The maintained device information includes, for instance, device identity, address, status (e.g. idle, active, etc.), capability (e.g. single slice capable device, multiple-slice capable device, etc.), device type (e.g. smartphone, sensors, vehicle, etc.), resource allocation (e.g. bandwidth, data rate, latency, etc.), connectivity status (e.g. connected via cellular network, connected via non-cellular network), location information, session information, associated slice, etc.

The network information includes, access network specific configuration parameters, slice specific information.

3.3.4 Interfaces to Other BBs

3.3.4.1 CM-Device

This interface is used for non-access stratum related C-plane messages exchange between device and CM.

3.3.4.2 CM – AF

This interface is used for CM to exchange access related signalling messages with AF, as well as receive access network related information (e.g. capacity, configuration setup, etc.) from AF. Via this interface, CM can also send access network related configurations to AF.

3.3.4.3 CM – SAM

This interface is used for CM to request subscriber data authentication related actions from SAM. If secured procedures are required, CM obtains security key from SAM via this interface.

3.3.4.4 CM – MM

This interface provides device related information, access network status and update (that may be involved in mobility decision) to MM. This interface is also used to receive session/path update from MM, and relay such request to FM.

3.3.4.5 CM – FM

CM provides context information[3], slice information and device state information to FM via this interface. Moreover, CM also uses this interface to request FM to setup/update/delete flows for devices. CM can obtain D-plane state such as network load for slice management purpose.

CM and FM both require abstract view from the D-plane with different granularity. CM requires D-plane anchor endpoints view, and FM has a view of D-plane nodes that in between the anchor endpoints. There are two options for design the relation between CM and FM as well as corresponding interfaces as shown in Figure 5. For the first option, CM and FM connect to an adaptation function (which will be further introduced in Section 3.6), which translates the CM/FM' SBI semantics into D-Plane configuration. For the second option, only FM has SBI towards network controller, and CM obtains the D-plane anchor endpoints abstract view from FM. In this case, adaptation function may be part of FM or an external function in between FM and network controller. The pros and cons for the above mentioned options are analysed in Table 2.

Table 2: Pros and cons analysis for two options

	Advantage	**Disadvantage**
Option 1	FM can be designed as an optional Building Block. While, FM is used to configure path in between anchor endpoints to enable value-added routing-service, which can be considered as optional. Without using FM, default rules in the D-plane nodes can also be used to establish path in between anchor endpoints.	CM needs to have and maintain SBI towards network controller.
Option 2	While CM does not have SBI towards network controller, which leads to simpler interface design for CM.	FM is a compulsory Building Block, which has to be existed for all scenarios.

[3] If context awareness sub-function in CM will be designed as an independent Building Block in future, this information will be provided by context awareness Building Block.

Figure 5: CM and FM interface relation illustration

3.3.4.6 SouthBound Interface (SBI) towards Network Controller in D-plane

In case option 1 design choice (mentioned in the above sub-section) is selected, CM has a SBI towards network controller. On this interface, CM retrieves abstract view on D-plane anchor endpoints, e.g. anchor endpoints topology, resource capability and availability, etc. Via this interface, CM also configures the anchor endpoints on the D-plane.

3.3.5 Required sub-functions

3.3.5.1 Network access control and configuration (NACC)

CM is the first contact point for the core network towards to a device. It invokes authentication and authorization for a device together with SAM Building Block. This sub-function facilitates a device to access to the network if it has sufficient credential, for instance allocating routable address for the device, and it may also distribute network configuration parameters to the device.

3.3.5.2 Access Function Interface Control (AFIC)

Some access technologies are capable of providing different link layer status information (i.e. link layer notification) to network layer. The AFIC sub-function is responsible to terminate link layer transport connection between the device and the network, which could be used for detecting the network attachment at the network layer.

This sub-function is also responsible to collect access network information from AF, e.g. access link related parameters, access point address, link identifier, device location, and device configurations, etc. Such information could be further used by MM to make and optimize mobility related decisions.

If the access requests from different type of access network have different format, then this sub-function is responsible for translation them into a unified format. This AFIC sub-function will forward the requests to NACC for further processing.

AFIC is also responsible to support access switching related procedures.

3.3.5.3 Slice management (SM)

One CM may need to provide and manage one or more slices. This SM sub-function is used to manage and maintain slice-specific information.

- Slice based D-plane anchor point management

CM is responsible to manage the D-plane anchor endpoints as stated in Section 3.3.1.7. Therefore, different slices may have different D-plane anchor endpoints abstraction, which are obtained from SBI provided by network controller as stated in Section 3.3.4.6. After a device is authenticated by the network, SM is responsible to allocate D-plane anchor endpoints for this device, and invoke FM (if necessary) to allocate the path in-between the anchor points. All the slice-specific anchor endpoints related information is maintained in this sub-function.

- Slice based flow management

Slice specific bearer related request (e.g. setup, update, delete) in LTE content or general flow management is also processed in this sub-function.

- Inter slice mobility engine (ICME)

ICME manages slice specific mobility related information, i.e. for all other slices available at a session endpoints' location the capabilities matching the active endpoints characteristics and sessions demands according to the users' and his/her subscriptions' policy. ICME collects and analyses the available information from all slices and decides and trigger inter-slice mobility related procedures.

- Slice related information provisioning

This function provides slice related information to access networks, devices, or the other building blocks that require such information. Support slice related procedure like attach, handover, etc.

3.3.5.4 Context awareness engine (CAE)

This sub-function collects existing information from devices, access networks and core networks, and also derive extra information based on the existing information, and output the context to the related BBs. For instance, it registers the association between the address/identifier (e.g. IP address) allocated for a device and related network location information, e.g. access point address, connection identifier, etc. This function may also associate the device address with geographical location information (e.g. GPS info, tracking area identity list, etc.) and map to time zone and signalling a device time zone change associated with mobility.

3.3.5.5 Roaming management (RM)

Support inbound and outbound roaming[4].

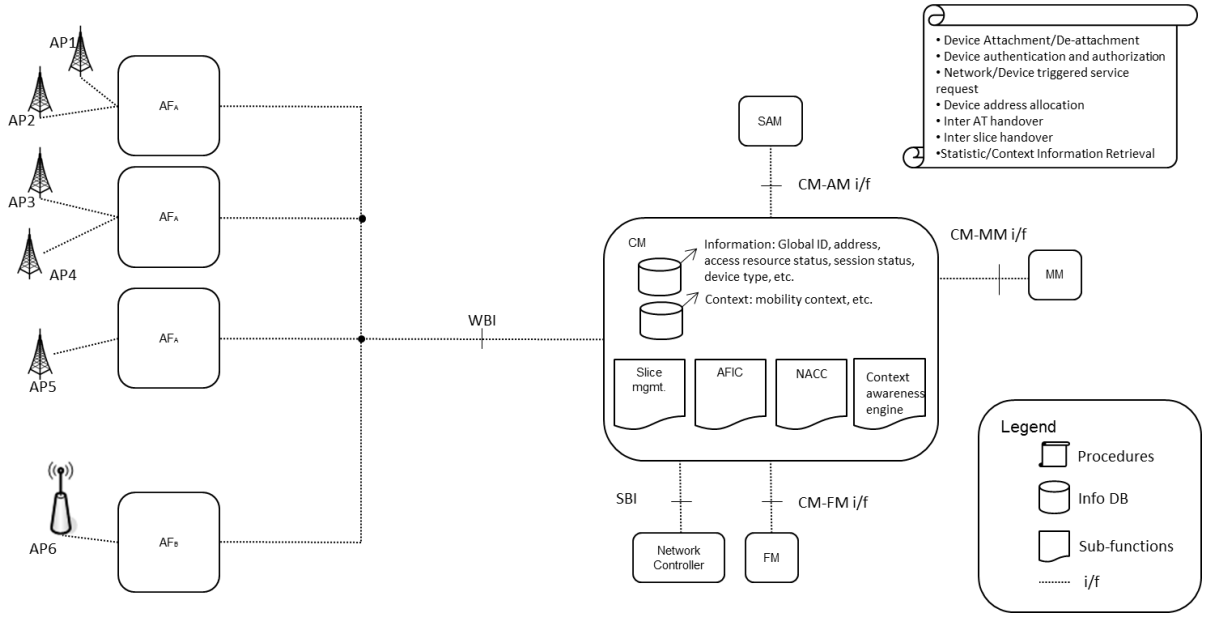

Figure 6: CM sub-architecture

[4] This is not the main focus of this project.

3.4 Security and AAA Management Block (SAM)

Communication networks provide access to billions of users and devices which store and exchange private and valued data. The data service usage keeps growing as the smart phones are likely taking the place of the legacy voice call phones and personal computers, connected devices as things with a low control foot print are more exposed to the public networks, and the future network architecture is likely driven by the SDN, they all expose new vulnerabilities and introduce new security challenges.

SAM is a Basic Building Block which accomplishes several functions in the scope of Security and AAA Management.

As justification for SAM being a stand-alone independent BB in CONFIG may serve the consideration that the AAA feature is not an optional BB. Even when using a low-secure authentication scheme, the SAM will be an integral component for the whole authentication and authorization procedures.

The SAM traditionally is in charge of the following tasks such as guarding against unauthorised Service usage (authentication of the end-device by the network and service request validation), provision of user identity, user data and signalling confidentiality (temporary identification and ciphering), provision of origin authentication of signalling data (integrity protection), and authentication of the network by the UE. The AAA functionality shall be access agnostic in a 5G control plane. Hence, the SAM needs to support a generalized AA(A) protocol for the connecting (consumer) nodes as well as providing an interface for other services to enable a trustful E2E relationship between the consumer, the network and the accessed service. Different AA-policies shall apply to different use cases and slices, e.g. in IoT slice for sensors only a low-secure authentication and authorization scenario may be required. This allows for different types of (granular) SAM functionality to be developed and applied related to protocols of different complexity.

Securing the network perimeter at the access segment and at the data network interface is also needed - to protect vulnerable points in the network but may leave the rest of the network open. The security in 5G has to be more comprehensive as to deal with the new threats, which are inherent to:

- The IP centric network architecture, vulnerable to service disruption, unauthorized access or data disclosure and modification attacks,
- The SDN model due to the logical centralization of control functions and to the decoupling of the control and packet forwarding functions. Security has to take into consideration of all layers of the SDN architecture, such as management, orchestration, application and the underlying virtualization and data center infrastructure.

The following section and related sub-sections explain the design considerations for SAM in terms of different tasks to accomplish.

3.4.1 Function Tasks

3.4.1.1 Identity management

Users need to be identified in a unique manner such as an IMSI provided by the USIM and stored in the HSS inside the LTE network components. The identity management has to be enhanced to securely reference devices (IoT) and applications (NFV). Different identity schemes may occur and the overall Identity Management needs to handle them accordingly.

3.4.1.2 Authentication, Authorization, Accounting, Auditing and Charging (AAAC)

In the overall 5G control plane, the SAM shall accomplish Authentication, Authorization, Accounting, Auditing and Charging (AAAC). These tasks are essential to provide a trustful and secure relationship between the accessing 5G (consumer) node and the provided 5G network slice. User, network and

service elements need to confirm that the communicating entities are the true entities they claim to be. Such Authenticating and authorizing the network is also required to enhance the security to the SDN architecture. Hence, also Controller entities, applications and network elements may use mutual authentication.

All attached nodes will authenticate and request authorization to access services that correspond to the C-Plane services. Interactions with the **CM** allow the exchange of required User and Device credentials. Hence the decision to permit attaching of the device can be pushed back towards the requesting CM.

Regarding authentication, network elements shall be able to authenticate the dynamically attaching network nodes in order to achieve high level of trust. In this case, authentication requests will be handled based on identity servers that are related to a subscription profile. This offers the possibility to use different identities for different services on a single consumer device. A possible protocol for that module is the EAP (Extensible Authentication Protocol) as a universal transport layer for authentication message exchanges (for fixed and mobile communication; EAP extensions could be in scope, too). Considering upcoming access technologies and their use cases for 5G, use case specific extensions of EAP may be applicable. Furthermore, the current LTE security mechanisms can be used in future networks as they are or even be enhanced, but it should always be carried over EAP. This could be used for different use cases like M2M/IoT, too.

Furthermore, SAML-based (Security Assertion Markup Language) signalling may be also used to resolve cross-authentication issues. In CONFIG, authorization will be achieved with an engine which is compliant with the eXtensible Access Control Markup Language (a.k.a. XACML). This engine constitutes an instantiation of an Attribute Based Access Control (ABAC) authorization scheme. ABAC scheme is proven to be superior when compared to competitive ones such as Role Based Access Control (RBAC) and Access Control Lists (ACL) since they are more flexible and more adaptable. According to the XACML scheme any access request has to be evaluated based on the evaluation of properties that correspond to three models:

a) the connected device model (i.e. the attached node);
b) the target resource (which corresponds to the control plane) and
c) the environmental context model. The authorization decision process is totally distributed; yet any decision will be forwarded to the requesting signalling units inside the network slice.

3.4.1.3 Access Agnostic (Single-)Sign-On

As addition, the SAM works in the scope of converged network signalling by having an agnostic view of the available access networks. Hence, a Seamless Sign-On between several Access possibilities is necessary to support the requirements of future 5G control plane.

For the communication of security data between operators and service platforms, web-based standards for SSO such as SAML (OASIS standard) is put in place. In this way, a user can use various services (paid or offered by the operator) by authenticating himself once, at network access level. It is ensured that visited web sites have only access to needed user information for providing and charging the service.

3.4.1.4 Trustful Relationship

This convergent AAA framework will offer well-defined AAA interfaces / protocols for service fulfilment in the scope of multi-tenant and multi-provider capable communication with various levels of authentication and authorization and ID/profile management.

There will be a common secure layer for negotiating the authentication methods to be used for several provider-based or vertical-based applications, such as provider owned service platforms or from OTT partners (trusted relationship between the agreed network partners).

3.4.1.5 Integrity, Confidentiality, and Availability on the Control Plane

Communications between network entities shall not be altered in undetected manner; the security has to generate keys for the access functions in the control plane (i.e., the **AF**) to compute the integrity code of each message in order to detect a possible modification of the message during the transport.

To prevent unauthorized entities from understanding and exploiting signalling and user data information, Key- and encryption functions are used to protect messages that are transmitted over the air or any other medium, and privacy protection shall be extended to the communications between layers in SDN architecture.

For guaranteeing the network and services availability, this block shall provide mechanisms to detect and mitigate threats. Proactive setting of security rules or reactive based on the collected information are only two possibilities for threat detection.

3.4.2 Related C-Plane Procedures

3.4.2.1 Device Authentication and Authorisation

The SAM covers procedures to ensure Authentication & Authorization of 5G network nodes in a reliable way. Based on the requirements and capabilities of the 5G network slice, the AA-functionality will perform the procedures according to the given security scheme, stored in a subscription profile for that specific device.

All of the device, user and service authentication and authorisation procedures consist of maintaining secret materials (shared key, calculation algorithms, sequence numbers and settings) dedicated to generate temporary information (such as authentication vector) for the authentication procedure, and provide a safe and hermetic computing environment (sandbox) when accessing to secret material. According the defined authentication procedures for devices and applications before granting the collaboration with another element, the device, user or service will be authentication and authorized.

3.4.2.2 User Authentication and Authorisation

Having a Device authenticated and authorized, End-Users shall also be Authentication & Authorization accordingly. Furthermore, SAM shall provide generation- and mapping-procedures to manage temporary identities to preserve the confidentiality of the user permanent identity and the mobility.

3.4.2.3 Service Authentication and Authorisation

The SAM covers procedures to ensure Authentication & Authorization of an End-User, Devices and Services in a reliable way. Based on the requirements and capabilities of the 5G network slice, the AA-functionality will perform the procedures according to the given security scheme, stored in a subscription profile.

Based on this, SAM will be an integral part of the connectivity setup and session maintenance. Setting up and maintain until the detachment of the entity will be part of the AM.

3.4.2.4 Secure C-Plane Manager

This procedure takes care of the confidentiality, integrity and availability management. Furthermore, it supports the access control between the Building Blocks inside the C-Plane.

3.4.2.5 Security Tokens Distribution

To ensure Single-Sign-On on different access networks or different services, the SAM may distribute

tokens to services and the underlying AF to support seamless service provisioning.

3.4.2.6 Identity - Locator Relationship

In 5G, there will be a separation from the Identity and the used Locator/address of the device. A numerous number of possibilities for such a mapping process will be addressed. Based on the subscription profile (including an Identification scheme, service usage profiles), a consumer may have several identities on a single device, or several locators using a single service. Other combinations may apply, too. Nowadays, the communication is driven by using a Domain Name System to resolve a specific address of a service. However, such mechanisms are applicable to address users, roles, devices, as well as services. This approach will lead to a dynamic and context aware Identity-Locator relationship.

The security module shall reliably manage and persistently maintain users, devices and applications identities which are unique key for the authentication procedure.

It shall also provide generation and mapping procedures to manage temporary identities to preserve the confidentiality of the user permanent identity and the mobility

3.4.3 Required Information

The information required by SAM BB to properly execute the function tasks as described in Section 3.4.1 covers the knowledge which identification and authorization the devices / endpoints and the sessions they are actively participating in will have based on the slice subscription profile. This information is also enhanced by maintaining several profile-to-role associations for a specific consumer.

As main information resource, the SAM BB requires the storage of subscription profiles for the 5G network nodes. Depending on the use case or the given slice, the subscription profile might have different characteristics and complexity (such as identity, secrets, used authentication algorithms as well as contracts).

All required data should be stored in a unified and scalable database to offer subscriber data management databases on a unique platform. The SAM will reuse 3GPP's UDC that splits the unified subscriber data management entity into two element types:

- the database which hosts subscriber and user profiles, and
- The front-ends which communicate with other network elements.

For accounting, it is necessary to store a type of Call-Data-Records (CDRs) to allow exact accounting per user, device, or service. Combinations out of that can be pushed to a business process, but will not be in scope inside this project.

3.4.3.1 Identities

The identities can appear with different characteristics:

- Permanent Identities: IMSI, mac, login name, etc.
- Temporary identities: GUTI, pseudonym, alias
- Identities can be maintained externally to the client modules

3.4.3.2 Secrets

Also different Secrets may be used with different complexity to authenticate a user, device or service:

- Permanent secrets: Shared keys, certificates, passwords, integrity codes, PIN codes, etc.
- Temporary secrets: derived keys, generated numbers or sequences, etc.

- Identities shall be maintained externally to the client modules.

3.4.3.3 Computation algorithms and libraries

To run a trustful and secure authentication process, milenage functions, key derivation functions need to be available at the SAM.

The key derivation can be provided by an external module to the requested client, but the data encryption and integrity protection functions shall be run within the client module.

3.4.3.4 Contracts

The provisioning of the users, devices and services is described in *user profiles, Access-Control-Lists (ACLs) with different complexity. Such profiles and ACLs can be maintained in a database external to client module.*

3.4.3.5 Topologies

If a secure communication between the BBs is required, the SAM can support the setup of such communication. However, it might be necessary to have knowledge about the current network topology or slice topology.

3.4.3.6 Application dependant

When securing the network via monitoring and threat detection, necessary information might be signatures, IP, DNS entries of the current network nodes.

3.4.4 Interfaces to Other BBs

3.4.4.1 SAM to Device

Provides interaction to assure identity, password and secret, as well as offers mutual authentication.

3.4.4.2 SAM to AF

Towards the AF, the signalling and data confidentiality as well as integrity protection using generated keys and computation functions will be ensured.

The confidentiality (CK) and the integrity (IK) keys are needed to protect signalling messages (K-NAS for instance) and the access bearer (K-eNB for instance). CK and IK keys computation are based on the authentication information, in EAP-AKA for instance, they are derived hierarchically from the original shared secrets.

The AF also needs functions and procedures from the SAM to encrypt and to protect the data from modification and to agree between the peers on the temporary keys to use. Furthermore, a policy exchange which access networks (such as in a roaming scenario) is done.

3.4.4.3 SAM to CM

The SAM provides access control list and the subscription profile to the CM, which controls the use of the network and services by the authenticated entity.

3.4.5 Required sub-functions

3.4.5.1 Unified Database for Identity Management

The database which maintains 5G IDs will cover user, device, service, and their assigned policies will offer a general subscription profile for the other C-Plane BBs (such as the **CM** or **AF**). Some extracted information can also be offered by towards the verticals, to offer a “personalised” service.

Such unified database shall also support non-3GPP Front-ends, and a more complex subscriber profiles (e.g., one subscriber can have many user profiles related to different accesses and services, but also to different persons i.e. kids using networks/services with limited rights).

Inside such a unified database, the required data exchange will cover the identification of the user, temporary identities, authorization, accounting data and other added value data such as location, device features, etc.

3.4.5.2 Authenticator

The Authenticator is the main part inside the authentication process. As possible protocol for that purpose, EAP (Extensible Authentication Protocol) can be used as a universal transport layer for authentication message exchanges (for fixed and mobile communication; EAP extensions could be in scope, too). Considering upcoming access technologies and their use cases for 5G, use case specific extensions of EAP may be applicable. Furthermore, the current LTE security mechanisms can be used in future networks as they are or even be enhanced, but it should always be carried over EAP. This could be used for different use cases like M2M/IoT, too.

Offering high-layer authentication methods is also in scope of the SAM, e.g., to support single-sign-on and web-based seamless service consumption.

3.4.5.3 Single Sign-On

This sub-module is used to provide the Task “Access Agnostic Single Sign-On” which provides functionalities to use various services by authenticate once.

3.4.5.4 Security Monitoring

This sub-function runs procedures to monitor the availability of other C-Plane modules as well as checking the integrity between the network entities.

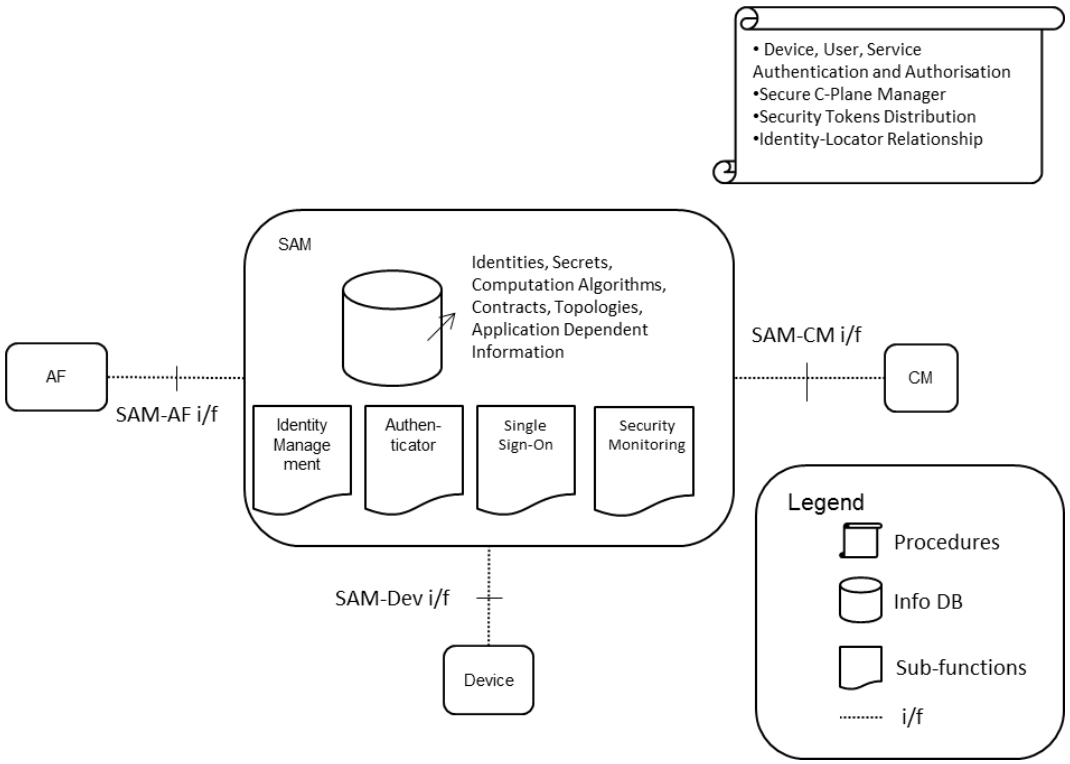

Figure 7: SAM sub-architecture

3.5 Mobility Management Block (MM)

Mobility Management (MM) is seen as a basic building block for deciding, initiating, and maintaining all major issues of a connection and the related active sessions which are impacted by a change in the endpoints of the connection (i.e., the end device or interface in the end device and the so-called corresponding node which may be a fixed host, e.g. content data server, or another end device). Such mobility events may be caused by movement of the user with his/her terminal equipment at specific speed out of and into the coverage area of an access domain, but also occur due to change in propagation conditions or local access network load. While the latter aspects may in general be handled by the access control network functions which do 'regular' mobility control (inside same access domain) and therefore are out of scope here, a feedback on relevant change in connection parameters could be considered also by the core control plane, especially if a change in slices or between fixed and cellular network is included.

In addition also changes in the end point itself for an ongoing session are included here e.g. a switchover between a handheld device and a locally fixed screen for displaying an active video transmission or between two devices in case the active one is experiencing battery drainage.

MM here is in charge of tasks which will enable 5G to extent currently restricted mobility capabilities in 4G-EPC. Thus in addition to decide on and steer Handover (HO) execution (in other cases than mentioned above where HO is handled within an access technology or an access domain autonomously) MM will enable 5G to feature:

- seamless inter Access Networks mobility with session continuity (e.g. same or different access technologies under same or different operators administrative domain);
- slice-specific mobility schemes (e.g. for unicast, multicast or broadcast communications) – see also [12][13];
- mobility patterns based schemes (e.g. state change for plurality of end devices such as in public or individual transport/traffic scenario)

An open question is whether and how the CONFIG MM concept has to deviate from existing 3GPP and (nearly seven years old) State-of-the-Art by ITU-T/NGN as described in [14].

As justification for MM being a stand-alone independent BB in CONFIG may serve the consideration that the mobility feature is an optional feature especially for fixed mobile converged 5G slices. For slices not supporting mobility (such as serving e.g. the residential/fixed broadband access use case), CM shall directly interact with AF without involving MM since no mobility events impact this service and paging and location tracking are unnecessary. This requires MM to be decoupled from CM and paging and location tracking being sub-functions of MM.

Mobility within 5G control shall be access agnostic: MM procedure shall be triggered towards/from AFs for any access technology supported by 5G (e.g. location update, paging). This requires MM to be decoupled from AF.

Different mobility support policies shall apply to different use cases and slices, e.g. in IoT slice for sensors only a nomadic mobility scenario may be required. This allows for different types of (granular) MM to be developed and applied related to protocols of different complexity. The instantiation of MM can be mobility scenario dependent (e.g.: for low mobility multiple distributed anchor and processing nodes, for high mobility few centralized nodes shall prevent too frequent handovers). This requires MM to be decoupled from CM and FM.

The following section and related sub-sections explain the design considerations for MM in terms of different tasks to accomplish.

3.5.1 Function Tasks

3.5.1.1 Mobility related events handling

MM is the CP entity that is handling Mobility related events at Core Network Side which generally includes all kinds of device or interface handovers between access domains (i.e. set of Access Nodes, e.g. Radio Head clusters) whereas those within the same domain are managed by a local mobility management on Access Function level and therefore agnostic for the core domain.

Device handovers among homogeneous/heterogeneous AFs (i.e. different AFs of same or different access network belonging to the same slice but are geographically or technically separated) may be handled within a hierarchical AF agent which is only notifying the MM of the HO or by MM agents within the ANs of the slice.

Handover of an ongoing session among different devices (e.g. see FMC Use Case 1) have to be controlled by the core MM on request of the user or proposed by the core MM (e.g. after a context trigger indicating the availability of a suited second device) to the user and executed after user acknowledgement.

Device or session inter-slice handovers may be required exceptionally (e.g. in case of unavailability of the foreseen slice and a high priority of the active service/session thus requiring instantiation of the session within a new slice depending on the valid policy). Such an event currently has low priority in the project, moreover in this cases the EastBound Interface (EBI) between different CONFIG domains might be included.

3.5.1.2 AN mobility policy enforcement

This task is related to match service-specific mobility demands (as kind of QoS) with session performance capabilities of the established connection. E.g. a slice or a service requires a specific level of mobility support (e.g. session continuity or endpoint reachability) on the one hand whereas the access technology is able to provide a degree of mobility in terms of endpoint movement support (e.g., none, low, medium, high) .The granted mobility support (e.g. in terms of subscription or slice specific policy or Service Level Agreement, SLA) shall be enforced by MM by proper selection of mobility decisions (e.g. type of Handover).

3.5.1.3 Device Location Tracking

MM has a global view of device and access network resource related information. For basic connectivity the Access Domain Identity together with the provided capabilities is sufficient to locate the device. In case of higher level performance demands (e.g. low-latency or very high bandwidth) a higher granularity of location is provided on-demand: e.g. availability of edge cloud resources to enable local processing at low delay or access capacity bundling via multiple connections available in the same region (hot spots). Tracking updates become necessary in case of higher impact on transport data path – e.g., switching to another CN node as endpoint of the data path flow to be managed by FM. Depending on the application needs and technological constraints the location information may be coded in terms of additional identifiers for e.g. tracking/paging area, current (access) point of attachment and require also IDs for session identification and endpoints, i.e. end devices or end device interfaces.

3.5.1.4 Device paging

In addition to traditional paging of idle devices in up to LTE technologies in 5G a higher separation of access and core domains is envisaged. Different access networks support different types of end devices – ranging between fixed (exhibiting no or at most sporadic - discrete - location change) and moving at different speeds (at continuous frequent location change). Therefore they provide location information at different granularity and need corresponding degree of paging feasibility only.

Furthermore in 5G some (low cost) types of device nodes such as sensors in IoT scenario may be energy constrained due to low battery power. To save energy these may be put in dormant state in case they are not actively participating in a session. Triggered by a (mobility) event (e.g. session set-up request from corresponding node) the endpoint has to be re-activated to enable session set-up.

MM in 5G needs to define an access and device independent (combined) paging and wake-up task which composed of different access and device specific procedures executed by the different supported Access Networks. E.g. starting from last known location area and depending on time-dependent predicted current location the paging command seeks to find, address, attach, and (re-)connect the end device node as endpoint of a (revived or new) session. For static devices a proxy node may store the device state and react on behalf of it on the request – while concurrently waking up the device and retrieving required information.

Depending on the access technology and topology, the location information is known and stored at different (hierarchical) levels (e.g. network wide or on location/paging/tracking area granularity) and/or at different entities (e.g. local access and aggregation node, access router, or LMA, Local Mobility Anchor for PMIP-domain). The information shall be consistent with the treatment as described in section 3.5.1.3.

3.5.1.5 Interconnection between $AF_{initial} \rightarrow AF_{final}$

During endpoint movement and handover controlled by MM the data transmission to the former/old/prior AF has to be re-routed to the new/upcoming/current AF. In case that the AFs have no valid horizontal control interface nor data plane connection either such a control interface and/or data plane path have to be provided by core CP MM BB. Default path may be via interface to core CP but a direct shortcut to be instantiated (depending on slice/session requirements) will be set up by MM. This task is related to Data Plane path switching between AF_initial and AF_final – whether this is within a single access domain or covers data paths in core or transport domain depends on whether same or different access technologies are involved and a hierarchy of AF is defined.

3.5.2 Related C-Plane Procedures

3.5.2.1 Location Tracking

This procedure defined in the Annex is executed to support DLT sub-function (see 3.5.5.2) to stay informed on all attached end devices' locations. Involved BBs are CM for provision of context information and the AF to retrieve the available location specific resources from.

3.5.2.2 Paging

The procedure defined in the Annex is required by DP sub-function (see 3.5.5.3) to activate an idle or dormant (with respect to core CP signaling) entity (e.g. on behalf of S-Plane initiated session request). Involved BB is the AF to derive and provide location information.

3.5.2.3 Mobility based Load Balancing

This procedure defined in the Annex initiates a network-based handover request. Depending on service performance demands, slice policies, and Access Network capabilities provided by CM (and retrieved from AF) MM reacts correspondingly, i.e. initiate horizontal intra- or inter-slice Handover via AF or vertical Handover via CM, followed by request to CM to initialize a session management / optimization procedure.

3.5.2.4 Handovers

The Annex differentiates between different types of Handover procedures in terms of intra-/inter-AT and –slice. MM sub-function 3.5.5.1 (MPE) checks the conformance with current session mobility

policy. Depending on HO complexity either only AF is involved (intra-AT HO) whereas in case of Inter-AT and inter-slice HO the control is delegated to CM. After HO execution at AF CM is requested to initialize a session management / optimization procedure. MM keeps track of the mobility state of the device.

3.5.3 Required Information

The information required by MM BB to properly execute the function tasks as described in Section 3.5.1 covers the knowledge where the devices / endpoints and the sessions they are actively participating in are topologically/geographically/logically located and where this data can be retrieved from within a specified time slot/frame.

In addition also the currently serving AFs (those to which devices are directly connected or via them they are attached to the system, e.g. relay nodes or other devices in D2D manner) shall be known to MM in terms of identity and/or (static or dynamic) location.

Finally the MM needs to know in advance of a HO decision what the capabilities and features of the AFs are (i.e. e.g. which capacity and QoS provision the underlying network(s) can offer).

These figures are stored in corresponding data bases as shown in Figure 8 as Info DB or are provided by other BBs via corresponding interfaces described in Section 3.5.4.

3.5.4 Interfaces to Other BBs

This section describes the foreseen interfaces to other BBs mainly in terms of message types to be exchanged in both directions. No MM-FM interface is needed since as described in Section 3.3.4.5 the CM interfaces FM in case of required DP reconfiguration which is not necessary during MM initiated events which do not comprise any change in core communication end points (blue circles) as shown in Figure 9 (in Section 3.6).

3.5.4.1 MM – Device

This interface towards an MM Agent at the end device node is only present in case that device centric (i.e. initiated and controlled) mobility is supported. The interface allows for exchange of device originated handover demands and to require handovers from the device in case the network decides on Mobility based Load Balancing as described in Section 3.5.2.3.

3.5.4.2 MM – AF

This interface is used in both directions to consider directly in mobility handling the access specific functions:

AF → MM:

- device location info (NAS piggybacking)
- device/session handover notification info
- inter-slice handover request (via CM) (tbd. for EastBound Interface, EBI, between different CONFIG core CP domains)

MM → AF:

- AN mobility policy enforcement info (high, low, nomadic mobility + Access Specific Rule Sets and its capabilities)
- QoS related session requirements
- device paging command (to reach a device, Location Based Services).

For this interface from AF point of view the provision of AN related (abstract) (attachment, HO) signalling messages and parameters coordinated with other CP BBs is foreseen, since involved

resources can be sliced/virtualized.

3.5.4.3 MM – CM

This interface is used for mobility related information exchange between MM and CM:

CM → MM:

- inter - slice and inter-AT handover information
- access Network Status/Condition update

MM → CM:

- inter – slice and inter-AT handover request
- intra-AN mobility event information

Note that changing an AN/AF may imply a change of conditions on U-Plane impacting QoS/QoE provisioning and thus also affect the required transport resource demand handled via FM.

3.5.5 Required sub-functions

The sub-functions of MM BB to provide the above described tasks and procedures are:

- Mobility Policy Enforcement
- Device Location Tracking
- Device Paging
- Mobility Management Agent (MMA) at AF

The MMA may be access technology specific e.g., an implementation for 5G, for EPS, for 3G, etc. and/or may exhibit domain/operator specific/dependent implemented features for different providers to offer a dedicated service capability as unique selling point.

The MMA may also be placed in device nodes.

Corresponding to the MM Agent at AF an MM Master (i.e. the MM BB) at core CP shall be present hosting the prior former three sub-functions.

A description of these sub-functions shall be specified in the following:

3.5.5.1 Mobility Policy Enforcement (MPE) sub-function

This sub-function matches the mobility policy which was decided on for a session and the endpoint based on the stored policy (e.g. in customer data base accessible by AM) to the current access performance as provided by AF. According to the description of task 3.5.1.2, MPE either invokes measures to adapt the performance to the session needs (e.g. by load balancing as described in Section 3.5.2.3) and – depending on the slice and session specific SLA – has to negotiate another service class (at lower QoE) or even deny session continuation.

3.5.5.2 Device Location Tracking (DLT) sub-function

DLT is directly related to procedure 3.5.2.1 to keep the state of a mobile session endpoint up-to-date to flexibly react to changing environments and connection quality. The frequency of DLT execution depends on the mobility policy which is agreed on within the slice or service.

3.5.5.3 Device Paging (DP) sub-function

DP is the sub-function responsible for addressing and calling a not connected device in case of to enable session set-up originating outside the device. DP starts the procedure described in Section 3.5.2.2 to find and 'wake-up' the session endpoint using the interface towards AF.

3.5.5.4 Mobility Agent (MA) sub-function

MA as a sub-function of the complete MM BB in the core is located in each AF to interface both the main module MM BB and react either on behalf of the device in case of network-based MM or with the MM client in the device in case of autonomous mobility-aware devices.

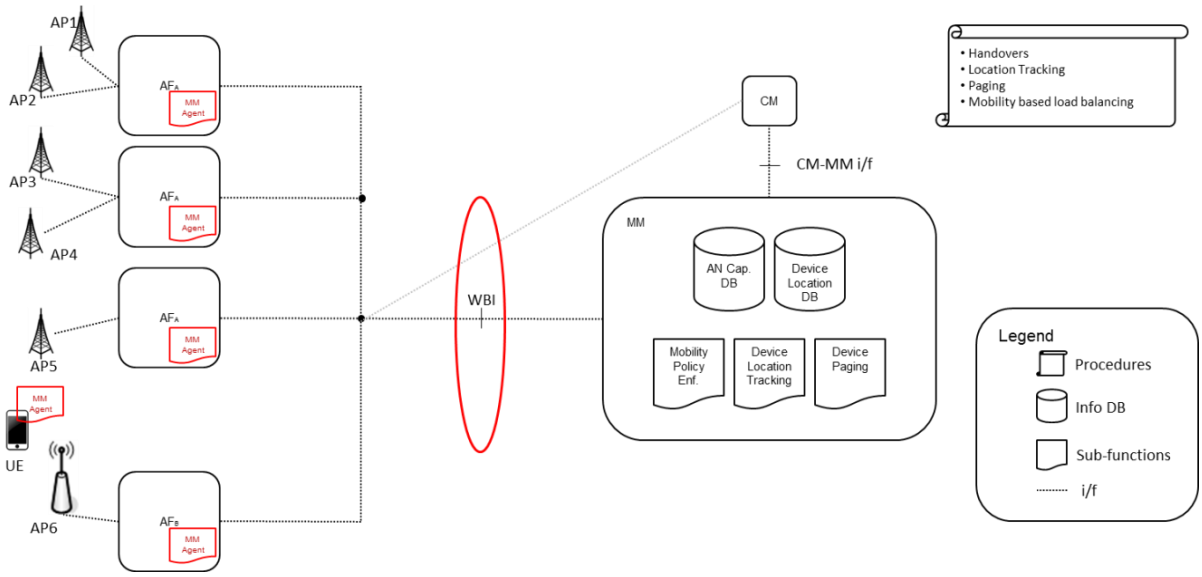

Figure 8: Mobility Management Building Block Sub-architecture

3.5.6 Open points on MM

Ongoing discussion covers merging between CM and MM building blocks as multiple sub-functions and required procedures focus on continuation of connectivity during mobility events. Consideration of more flexible sub-functions differentiating between connectivity without any mobility and discussed degrees of variability of both physical and logical end point location would reflect the required slice differentiation.

In addition the aspects of inter-slice handover and interfaces between MM and CM functions in both slices would be taken into account properly in the updated description of a CMM (Connectivity and Mobility Management) building block. Consideration of interfaces as described in Section 3.5.4 could ask for an additional inter-MM interface (located at different slices/domains) and also to handle communication between MM Agent (MMA) with proxy-like functionality located at each AF (and potentially also at device) and the MM Core component (MMC). Since the latter relation would be rather of master-slave character and not like between separate BBs such an interface presumably would not be required.

An originally proposed interface to SAM for exchanging security and AAA related information in case a mobility event (e.g. requiring new credentials or temporary identities to preserve a user's and end devices location privacy) is still under discussion and needs further studies. One way to get rid of such additional interface would be to retrieve these data from CM.

3.6 Flow Management Block (FM)

Flow Management (FM) is the block in the C-plane to control how data path flows are traversing the core – i.e. generally between gateways towards access domains and/or towards other domains or end points such as e.g. servers hosting application. In addition to controlling data paths, FM also manages the related procedures which involve establishing and reconfiguring data paths. FM needs to be an independent BB because it is the only block which has entire responsibility of fine grained data plane management. As such it has peering with a number of other BBs like CM, SM, and AF. From a business perspective it offers the potential of being implemented in different ways with

diverse features, hence the need of a separate BB. Furthermore the FM can have a distributed implementation which means it can be instantiated in multiple locations.

3.6.1 Function Tasks

3.6.1.1 Manage the D-plane

The primary task of the FM is to handle all tasks related to the management of the D-Plane. This involves computation, selection, establishment and release of forwarding paths. The information context plays an important role in the path selection and as such FM relies on input from the context aware engine. Suitable D-plane topology information as well as node context (capability, load, etc.) is to be exposed to the FM. Figure 9 depicts an exemplary view of the D-Plane at the FM, where the FM can treat D-Plane nodes differently. The C-Plane utilizes some D-Plane nodes (blue) to enforce advanced rules, such as for traffic steering, labeling, metering or traffic engineering, whereas other nodes (green) are solely used to enforce data to traverse a certain path as per the result of path computation.

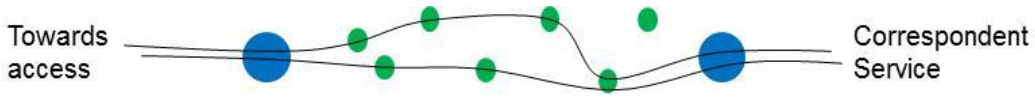

Figure 9: The role of FM is to manage only the green nodes

In an exemplary comparison with today's LTE architecture, the depicted two blue nodes in Figure 9 can represent a PDN Gateway and Serving Gateway respectively which enforce rules for bearer binding, chargeable event monitoring and metering, mainly to support functional operation, whereas the green nodes can be configured to enforce rules to route data flows on a particular path.

Service Function Chaining (for e.g. in the SGi-LAN) serves as further example to describe different treatment of D-Plane nodes from the FM. Nodes, which aggregate various rules to classify traffic for the assignment to a service graph, enforce a more complex set of rules (blue) compared to transport nodes (green), which forward flows towards a service function as per the specified service graph.

Extensibility in terms of sub-functions and southbound interface semantics is a key design objective for the FM to enable the enforcement of advanced rules in the D-Plane for future deployment, such as a dedicated D-Plane slice which adopts ICN/CCN paradigms for content distribution.

3.6.1.2 Enforce and manage QoS policies

This involves resource reservation for critical flows (time critical or life critical) and path management based on QoS profiles. This will involve interaction with other BBs such as AF to obtain information about the access network for QoS enforcement.

3.6.1.3 Integrate alternate transport technologies

The scope of FM is global in that it should be able to integrate the different transport technologies and hence should have necessary plugins to support this.

3.6.2 Related C-Plane Procedures

3.6.2.1 Data Plane Establishment

FM is involved in data plane established based on specific requirements. The forwarding path definition engine and flow management decision engine are the prime sub-functions involved in this procedure however if the underlying data plane is heterogeneous then alternate transport technology integrator can be called as well. FM will also be involved in this procedure is there is a device triggered or network triggered service request.

3.6.2.2 Data Plane Reconfiguration

The forwarding plane monitoring engine sub-function as well as context information can report events which might require data plane reconfiguration. Furthermore handover be it inter-access technology or Inter-slice handover can result in data plane reconfiguration. Vertical handover is used to support device changes from one access network to another access network. If the access networks belong to the same slice, then vertical handover only triggers D-plane update without C-plane changes. If the access networks are in different slices, such vertical handover triggers slice switching, which result into C-plane and D-plane changes.

3.6.2.3 Data Plane Tear Down

The decision engine in the FM is primarily responsible for data plane teardown.

3.6.2.4 Handover

FM is involved in this procedure as it involves data plane reconfiguration.

3.6.2.5 Inter AT Handover

FM is involved in this procedure as it involves data plane reconfiguration.

3.6.2.6 Inter Slice Handover

FM is involved in this procedure as it involves data plane reconfiguration.

3.6.2.7 Device Triggered Service Request

FM is involved in this procedure as it involves data plane establishment.

3.6.2.8 Network Triggered Service Request

FM is involved in this procedure as it involves data plane establishment.

3.6.3 Required Information

FM keeps the following information

- Information about the communication endpoints.
- Network resources ((abstracted)
- Network Topology (abstracted)
- QoS Parameters (Delay, Jitter)
- QoS Profile Repository
- Flow /Node IDs, Flow state

In addition it needs the following information from other BBs for its operation.

- Context info.
- Access related information.

3.6.4 Interfaces to Other BBs

3.6.4.1 FM – AF

AF --> FM

- This interface is used to retrieve access network information in an abstract way. This information can in turn be used to optimize data path for e.g. to guarantee specific QoS needs.

3.6.4.2 FM – CM

CM --> FM

- Context information as the context awareness engine is assumed to reside in the CM.
- Device state information in the CM which can be used for flow optimization.
- The slice requirements and other related information.
- The mobility related events for e.g. change of anchor points will be communicated from MM to FM via CM as CM will be involved in this in any case.

FM --> CM

- As for the information flow to the CM, FM can feed it with the info about the D-plane state such as network load for slice management.

3.6.4.3 FM – SAM

FM --> SAM

- For flows that might be encrypted FM needs to communicate with SAM on this interface.

SAM --> FM

- On the other hand in case the D-plane needs to be encrypted, the SAM will enforce the keys and rules through FM.

3.6.5 Required sub-functions

The architecture of the FM building block is shown in Figure 10. It comprises of the following sub-functions.

3.6.5.1 Forwarding plane monitoring engine

The FM needs to have a mechanism to monitor the status of the underlying data plane. Say for example monitoring QoS parameters such as delay, jitter. This is accomplished by the forwarding pane monitoring engine sub-function.

3.6.5.2 Forwarding path definition engine

In order to setup the forwarding paths there must be an engine defining the forwarding paths based on relevant metrics.

3.6.5.3 Flow management decision engine

This sub-function is the brain of the FM in that it models the input information and takes the necessary actions to be presented to the data plane underneath via the SBI.

3.6.5.4 Alternate transport technology integrator.

A typical data plane can be quite heterogeneous in that it can have legacy nodes or SDN based nodes with separate data and control plane. The role of this sub-function is to integrate alternate transport technologies.

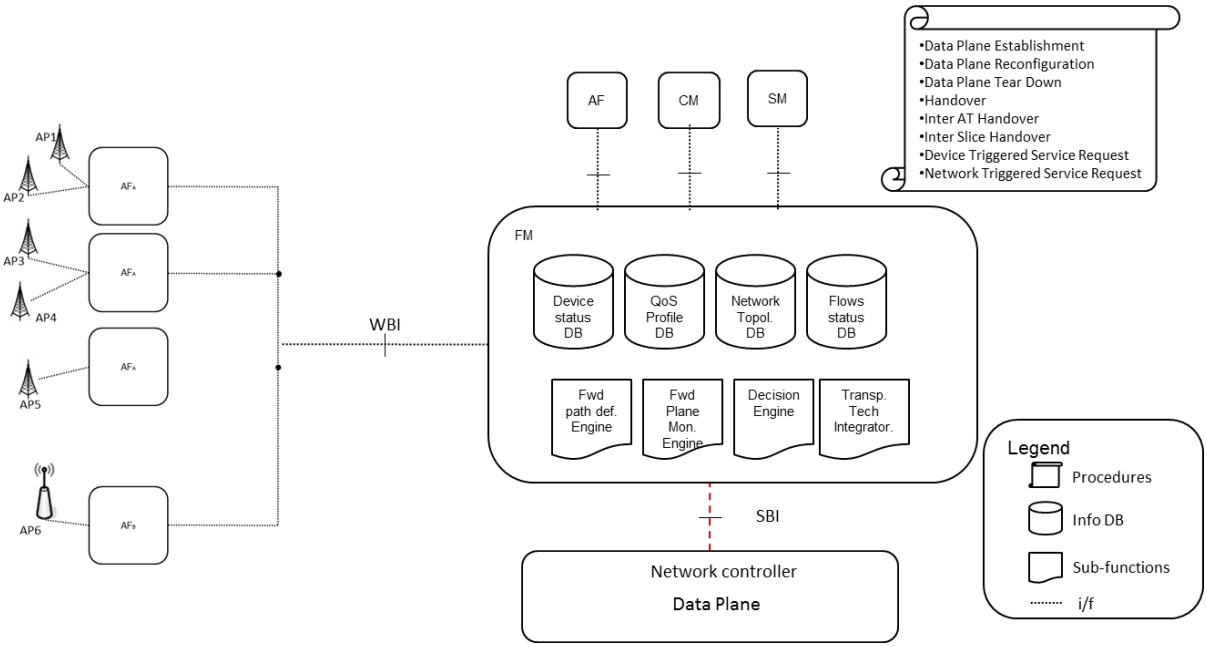

Figure 10: Architecture of Flow Management (FM) building block

3.6.6 SouthBound Interface (SBI) towards the D-plane

The FM needs to have an abstract view of the network underneath. Abstraction of D-Plane topology, either on a per-slice basis or a shared D-Plane, and of D-Plane node context can be enabled by a Network Controller. To remain independent of a particular D-Plane technology and its configuration particularities, the FM utilizes common semantics on its southbound interface to have the full control to configure relevant rules on the D-Plane and to receive notifications or queries from the D-Plane. The CONFIG project currently assumes an adaptor function as shown in Figure 11 to terminate the FM's southbound interface. The adaptor can be co-located or be distant to a Network Controller and may utilize a single or a variety of protocols/interfaces to collaborate with a Network Controller and other associated applications. The adapter appears as a data plane entity to the C-plane while it appears as a control plane entity to the D-plane. Further the adaptor supports multiple connections to multiple instances of an FM (as the different instances can be distributed in the network) and potentially to BBs of a different type. For instance CM is the BB which requires configuration of endpoints. This can be achieved by CM directly talking to endpoint nodes on SBI via the adapter. This option makes it possible to configure a slice which might not require FM for example for use-cases for which the default best-effort route between the endpoint might is enough.

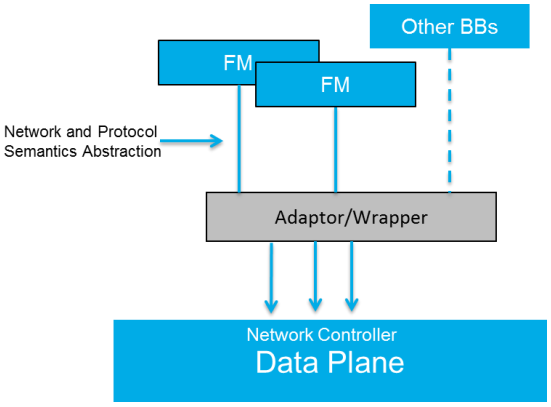

Figure 11: A generic adaptor for data plane abstraction and rules enforcement

The assumed functional architecture between a Network Controller and the BBs can be extended and deployed in different ways. E.g. to aggregate protocol endpoints from multiple BBs and resolve

conflicts, or to provide BB-specific abstraction and protocol semantics, an additional function serving as proxy can be existent in between an FM and an adapter, which is exemplarily depicted in Figure 12 and denoted as BB-specific Network Controller (FM Network Controller).

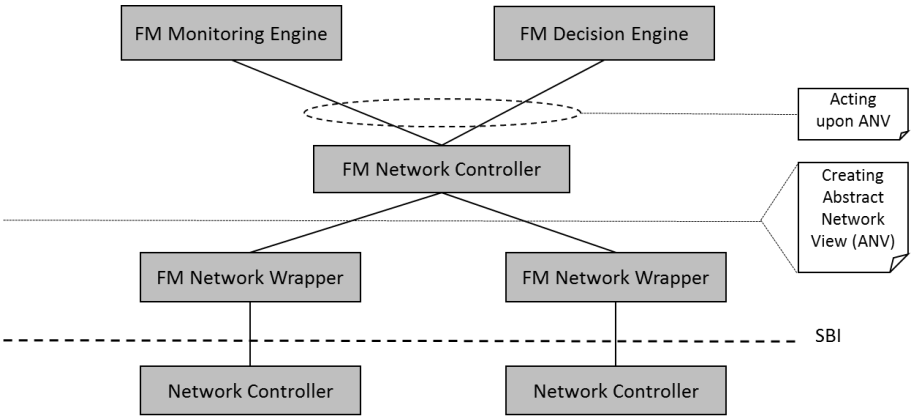

Figure 12: FM specific data plane abstraction

It needs to be highlighted that if FM is assumed to be the only BB with the interface towards the data plane then all other BBs need to perform data plane dependent operations via FM. Examples of data plane dependent operations by other BBs are anchor point configuration by CM, keys and rules enforcement by SAM in case D-plane needs to be encrypted. This makes FM a mandatory and almost always present BB in all scenarios. However another option can be that BBs which need to insert rules in the data plane talk directly to the data plane via SBI. For example CM can configure the communication endpoints and there can be a default route between these end points. For some cases this basic connectivity with default route will be enough and as such FM is not needed. However in case fine tuning of paths is required then the FM can come into play and select the appropriate nodes based on some metric say load, QoS, congestion, other context. Also for advanced cases e.g. SFC or ICN/CCN, the FM may be included to enforce particular rules in the D-Plane to enable these cases.

4 5G West Bound Interfaces

4.1 WBI Model

Figure 13 describes the reference model for the definition of the West Bound Interface. It derives from an extensive state of the art analysis (see Section B.1) of wireless and wireline access network technologies for which the CONFIG aims to provide a converged control plane.

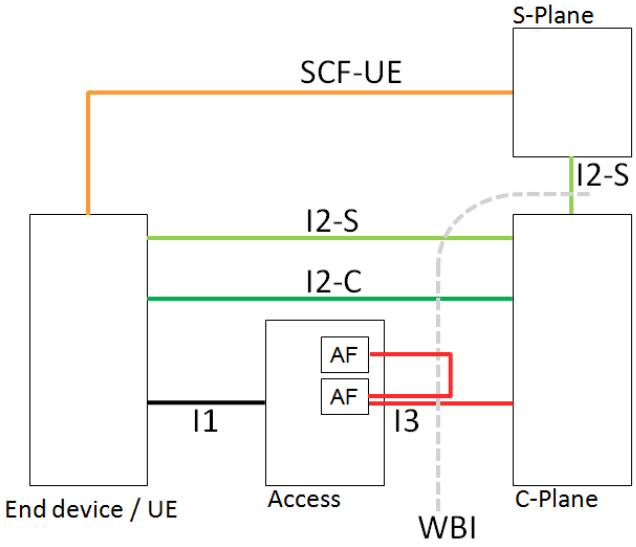

Figure 13: WBI reference model

The block *C-Plane* refers to the converged CONFIG control plane including the building blocks CM, MM, FM, and SAM. The block *Access* refers to access specific building blocks in the scope of CONFIG, in this document referred as AF. The *End device* may be a machine type device (in IoT or sensor scenario), an end user device or a customer premises device (CPE) that handles control plane signalling with the access network and the C-Plane. *S-Plane* refers to a generic service plane (out of the scope of CONFIG) that provides on line services to end devices.

The interface SCF-UE (Service Control Functions – End Device/UE) involves specific signalling for the establishment of service sessions exchanged between applications running on the end device and applications in the S-Plane. More details about SCF-UE interface are in Section 4.2.

In any case, a service running in the device and/or in the S-Plane requires the establishment of Data Plane (DP) sessions. Interface I2-S is meant to request DP session establishment. I2-S signalling can be originated by the End device or by the S-Plane. Requirements and state of the art for interface I2-S are described in Section 4.3.

Control plane signalling for network attachment and mobility may involve the mediation of Access functions or may not. In the second case the End device performs direct signalling with the C-Plane on interface I2-C, described in Section 4.4. If Access function mediation is needed, the End device performs access specific signalling on interface I1 (not in the scope of CONFIG) and the Access function handles C-Plane signalling on interface I3. The signalling may involve C-Plane building blocks and/or other AFs, as shown in Figure 13.

Interface I3 is also meant for location tracking and reachability for end devices that does not handle direct signalling with the C-Plane for those purposes, as well as for access function configuration. More details on interface I3 are provided in Section 4.5.

4.2 SCF-UE Interface

The main reference for this interface, which is not in the scope of the current study, is the interface between the CPE and the Service Control Functions introduced by ITU-T NGN specifications Y.2111 [20] (see Appendix I Section B.1.1). Interface SCF-UE may involve control signalling for a wide variety of applications, spanning from session oriented applications (e.g. legacy voice, VoIP), basic internet access services (e.g. HTTP, email), streaming (e.g. VOD and RTSP based video systems), gaming, peer-to-peer file trading as well as new services that may arise in the 5G context (mission critical Machine Type Communication, Intelligent Transportation Systems, etc.).

4.3 I2-S Interface

I2-S refers to access agnostic signalling that applications in End device or S-Plane perform with the C-Plane to establish DP sessions. In principle, the I2-S end point building block within the C-Plane is the CM. Exception are all service specific SA4C (Security, AAA Auditing and Charging) related procedures which are controlled by SAM.

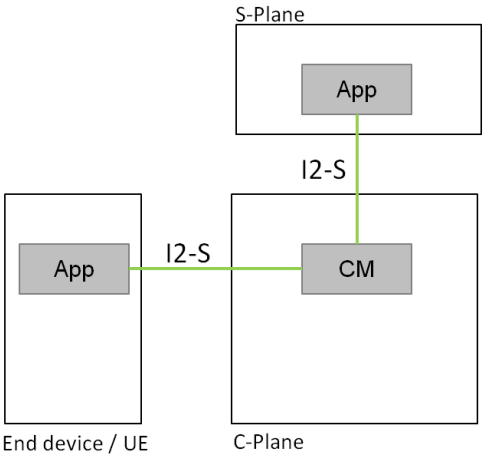

Figure 14: Interface I2-S

The main state of the art reference for this interface are the QoS control procedures described by ITU-T NGN Y.2111 ([20], Section 10.1 “Procedures for QoS control”), which is initiated by Service Control Functions (i.e. Applications) in the Service Stratum, the equivalent of our S-Plane. Differently from Y.2111, in our case the Application triggering the session establishment can be both in the End device and in the S-Plane.

We foresee two main types of I2-S procedures:

- Admission decision procedures: in this case the Application requests the CM an admission decision for a DP session. The CM determines if the session request can be admitted and replies to the Application on the I2-S interface. The CM does not establish the requested session. The CM may install the rules and reserve the resources needed to establish the session, but it does not activate them. The decision about the policy for reserving the resource can be based on device identity, device type and application type.
  The DP session for which the admission decision is requested may concern a different Application from the one that requested the admission. For instance, an Application in the S-Plane may request an admission decision for a session that will be requested by an Application in an End device (e.g. as guest, in the access network). Also vice versa/the other way round the S-Plane App may request to send unwished data (e.g. advertisement) to the UE but the resource for that session will be only granted if the UE confirms/acknowledges the action since the data transmission will waste/contribute to the users tariffed volume.

- Session establishment/modification/release procedures: the Application requests the establishment/modification/release of a session. In case of establishment or modification, the CM performs an admission decision. If the session establishment or modification was previously admitted, the CM performs straightforward the session establishment or modification.

Note: while it is immediate to establish an analogy of these procedures with 3GPP NAS (Non Access Stratum) procedures for service request, it is less immediate when they concern access networks like WiFi access points. In this case the I2-S procedures must be interpreted as procedures to establish e2e sessions with guaranteed QoS.

Two state of the art references for the definition of I2-S are:

- Interface Rh' in ITU-T Rec. Y.2111 [20] between PD-FE (Policy Decision Functional Entity) in RACF and CGPD-FE (CPN gateway policy decision functional entity) in CPN (Customer Premises Network). This Reference Point conveys information on QoS handling, priority handling and resource usage.
- Interface Rh in ITU-T Rec. Y.2111 [20] between PD-FE in RACF and CGPE-FE in CPN. Via this Reference Point policy decisions are pushed to CGPE-FE and admission decisions are requested from PD-FE. More information on the state of the art is provided in Appendix Section B.1.1.
- The reference point between AF (Application Functions) and PDP (Policy Decision Point) in Broadband Forum TR-134 [27]. More details are provided in Appendix Section B.1.5.

4.4 I2-C Interface

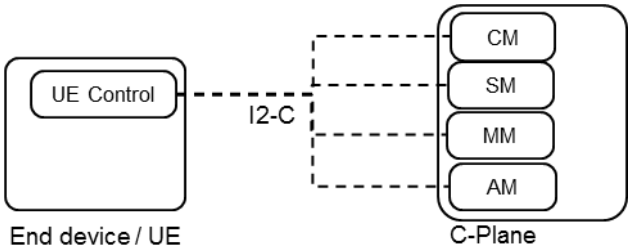

Figure 15: Interface I2-C

I2-C refers to the interface for access and device type agnostic signalling between the control entity within the End device and the C-Plane required for network attachment and mobility, and for device configuration. The sub-modules of CM consider device state, address, support configurations required depending on states of both the device and the network in correlation to the session demands, and maintain corresponding context information. SAM arranges for service and network access unaware AAA functionality and security associations (e.g. in case of roaming) whereas MM modules communicate with client-based mobility aspects (e.g. user initiated handover).

This interface handles all end device configuration related information and commands. Details will be elaborated in the corresponding BB description.

State of the art references for the definition of I2-C are:

- Interface S2c in 3GPP TS 23.402 [15]. This interface provides the user plane with related control and mobility support between UE and the PD Gateway when the UE is connected via trusted non-3GPP or untrusted non-3GPP access networks. To be noted that interface S2c issues requirements to the UE, which must support DSMIPv6 (Dual Stack Mobile IPv6) [17]. More information on the state of the art is provided in Appendix Section B.1.2.
- Interface S14 in 3GPP TS 24.312 [16]. This interface introduces in the evolved packet core (EPC) the Access Network Discovery and Selection Functions (ANDSF) entity. The ANDSF

assists the UE to discover non-3GPP access networks and provides the UE with network selection policies. More information about ANDSF and WiFi access point is provided in Section B.1.3.

- Interface R2 in draft IEEE 802.1cf (OmniRAN) [19] for logical control (e.g. authentication procedures) between UE and subscription service in core control. More information on the state of the art is provided in Appendix Sections B.1.4.

4.5 I3 Interface

The I3 interface between access network or access control network functions (AF) and the C-plane handles network attachment and mobility as well as access network configuration. Generally spoken all necessary procedures to be executed without requiring direct interaction or participation from the device are using this interface. MM modules directly interact with network-based MM agents in the access networks to provide session continuity without end user awareness.

Direct control plane interactions among AF building blocks, for instance for what concern mobility management, are also in the scope of I3.

At the state of the art there are several references for the definition of I3:

- Interfaces between access specific network elements and PDN GW: interfaces S2a (for trusted non-3GPP access networks), S2b (for untrusted non-3GPP access networks) and S5 (for 3GPP access) in 3GPP TS 23.402 [15] for IP address allocation and to provide user plane with related control and mobility support; all the three interfaces can be GTP or PMIP (IETF Proxy Mobile IPv6) [18] based. More details in Section B.1.2.
- Interfaces between access specific network elements and HSS or AAA in EPC: interfaces STa (for trusted non-3GPP access networks), GSWa and SWm (for untrusted non-3GPP access networks) and S6a (for 3GPP access) in 3GPP TS 23.402 [15]. More details in Section B.1.2.
- Interfaces between access specific network elements and PCRF in EPC: interfaces Gxa (for trusted non-3GPP access networks), Gxb (for untrusted non-3GPP access networks) and Gxc (for 3GPP access) in 3GPP TS 23.402 [15]. More details in Section B.1.2.
- Interface between access network control and subscription service in OmniRAN/IEEE 802.1cf: R4 (or R3s) for AAA and policy functions is proposed in [19]. More details in Section B.1.4.
- Interface between access network control and Access Router (core network, i.e. e.g. Config GW towards Access Domain) in OmniRAN/IEEE 802.1cf: R9 (R3c) representing a logical interface for control and management functions is proposed in [19]. More details in Section B.1.4.
- Interface between PDP (Policy Decision Point) and Policy Enforcement Point (PEP) in BBF TR-134 [27]. More details in Section B.1.5.

5 Inter BBs Interfaces

This section summarise the Inter BBs interfaces as shown in Figure 16, which are addressed by each BB as described in Section 3.

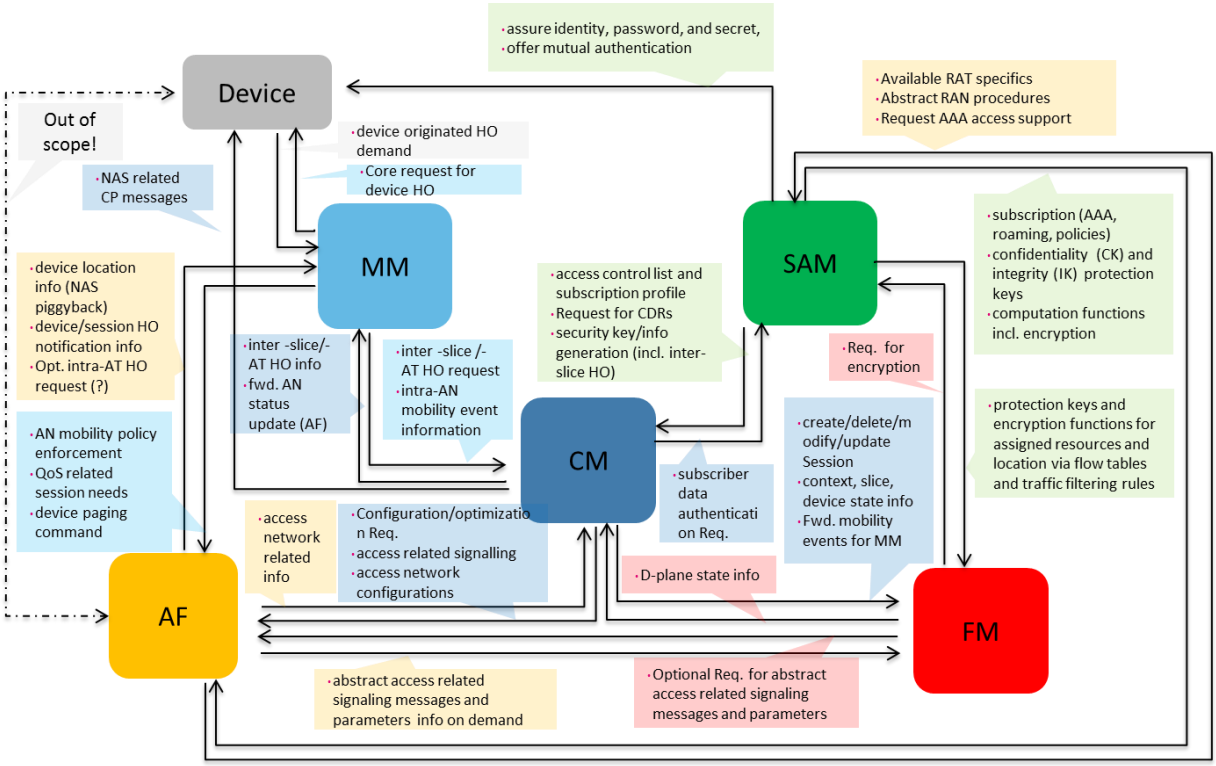

Figure 16: Summary of the Inter BBs interfaces

Annex A List of C-Plane Procedures

This Annex includes a reference list of the key 5G control plane procedures relevant for CONFIG architecture design.

A.1 Device Attachment

Via Device Attachment, an authorised device is authenticated, allocated an address and associated to a basic (i.e. with no QoS) D-plane forwarding path (for a given slice).

It includes:

- *Device Address Allocation*
- *Device Authentication and Autorisation*
- *Data Plane Establishment*

A.2 Device Detachment

Via Device Detachment, an attached device is de-allocated its address and its basic D-plane forwarding path is torn down (for a given slice).

It includes:

- *Data Plane Tear Down*

A.3 Device Address Allocation

Via Device Address Allocation, an address is allocated to a device (for a given slice).

A.4 Device Authentication and Authorisation

Via Device Authentication and Authorisation, a device is authenticated and its credentials to perform the action it is requesting are verified (for a given slice).

A.5 User Authentication and Authorisation

Via User Authentication and Authorisation, a user is authenticated and its credentials to perform the action it is requesting are verified.

A.6 Service Authentication and Authorisation

Via Service Authentication and Authorisation, a service is authenticated and its credentials to perform the action it is requesting are verified.

A.7 Secure C-Plane Manager

This procedure takes care of the confidentiality, integrity and availability management. Furthermore, it supports the access control between the Building Blocks inside the C-Plane.

A.8 Security Tokens Distribution

This procedure distributes tokens to services and the underlying AF to support seamless service provisioning.

A.9 Identity – Locator Relationship

A procedure to manage and map temporary identities to preserve the confidentiality of the user

permanent identity and the mobility

A.10 Device Triggered Service Request

Via Device Triggered Service Request, an attached device requests the establishment of a specific D-plane forwarding path.

It includes:

- *Service Authentication and Autorisation*
- *Data Plane Establishment*

A.11 Network Triggered Service Request

Via Network Triggered Service Request, the network requests the establishment of a specific D-plane forwarding path for an attached device.

It includes:

- *Service Authentication and Autorisation*
- *Data Plane Establishment*
- *Paging or Device Wake Up (optional)*

A.12 Data Plane Establishment

Via Data Plane Establishment, a specific (i.e. with QoS) D-plane forwarding path is set up.

A.13 Data Plane Reconfiguration

Via Data Plane Reconfiguration, a specific (i.e. with QoS) D-plane forwarding path is modified (i.e. QoS profile changes, or D-plane configuration changes).

A.14 Data Plane Tear Down

Via Data Plane Tear Down, a specific (i.e. with QoS) D-plane forwarding path is removed.

A.15 Handover

Via Handover, an attached device associated to an active specific (i.e. with QoS) D-plane forwarding path changes the access point it is connected to.

It includes:

- *Data Plane Reconfiguration*

A.16 Inter AT Handover

Via Inter AT Handover, an attached device associated to an active specific (i.e. with QoS) D-plane forwarding path changes the access point and the access technology it is connected to.

It includes:

- *Data Plane Reconfiguration*

A.17 Inter Slice Handover

Via Inter Slice Handover, an attached device associated to an active specific (i.e. with QoS) D-plane forwarding path changes the slices it is connected to.

It includes:

- *Data Plane Reconfiguration*

A.18 Location Tracking

Via Location Tracking, the network updates the location information of an attached device.

A.19 Location Update

Via Location Update, an attached device triggers the update of its location information at network side

A.20 Paging

Via Paging, the network triggers the re-activation of an attached but idle device, which location information is imprecise or outdated, and for which data are to be delivered.

A.21 Device Wake Up

Via Device Wake Up, the network triggers the re-activation of an attached but idle device, which location information is known, and for which data are to be delivered.

A.22 Mobility Based Load Balancing

Via Mobility Based Load Balancing, the network triggers Handovers and/or Inter AT Handovers and/or Inter Slice Handover as a consequence of network load conditions.

A.23 Statistic/Context Information Retrieval

Via Statistic/Context Information Retrieval, the network collects information on the operating network resources and devices.

Annex B Prior Art Analysis

B.1 West Bound Interface

B.1.1 ITU-T NGN

The two flow diagram scenarios depicted In ITU-T Y.2111 [20] constitutes reference prior art for interface SFC-UE in our framework.

Scenario 1 (Figure 17) is the QoS resource control scenario in *push mode*, meant for all types of CPE: CPE type 1 does not have any QoS negotiation capability (e.g. vanilla soft phone, gaming console), CPE type 2 supports QoS negotiation at the service stratum (e.g. SIP phone with SDP/SIP QoS extensions), CPE type 3 supports QoS negotiation both with the Service control function and the Transport functions (e.g. UMTS UE). In scenario 1, the CPE requests an application-specific service by sending a service request (1) to the SCF. The service request may or may not contain any explicit service QoS requirement parameters.

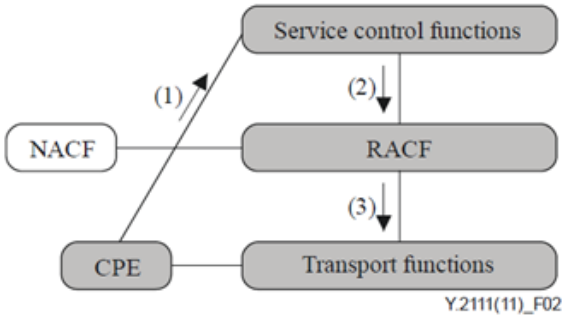

Figure 17: ITU-T Y.2111, flow diagram scenario 1

Scenario 2 (Figure 18) is the QoS resource control scenario in *pull mode*, supported only by type 3 CPEs. In this case the service request (1) goes to the Service control functions but the CPE may initiate a request with QoS information for resource reservation directly to the transport functions.

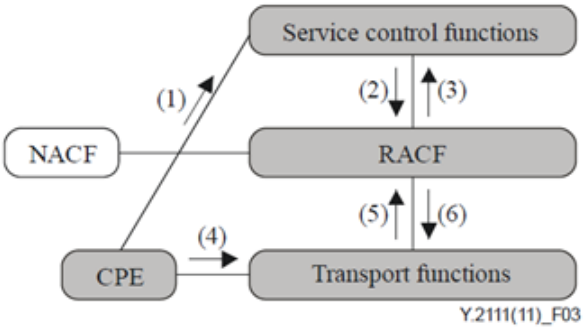

Figure 18: ITU-T Y.2111, flow diagram scenario 2

In the ITU-T NGN architecture [21] the service stratum is responsible for the application signaling, and the transport stratum is responsible for reliable data forwarding and traffic control. The RACF is the function that determines the availability of the resources and appropriately controls the network element. In Y.2111 [20] the RACF has two functional entities, as shown in Figure 19:

- The policy decision functional entity (PD-FE):
  - The PD-FE controls the policy enforcement functional entity (PE-FE) in the transport network;
  - The PE-FE (Policy Enforcement FE) is located at the edge or boundary of the regional

network. In embodiment, the PE-FE can be implemented in different forms such as session border gateway, CMTS, edge router, and so on.

- The transport resource control functional entity (TRC-FE).
  - The TRC-FE monitors the network topology and the resource state of the regional network.

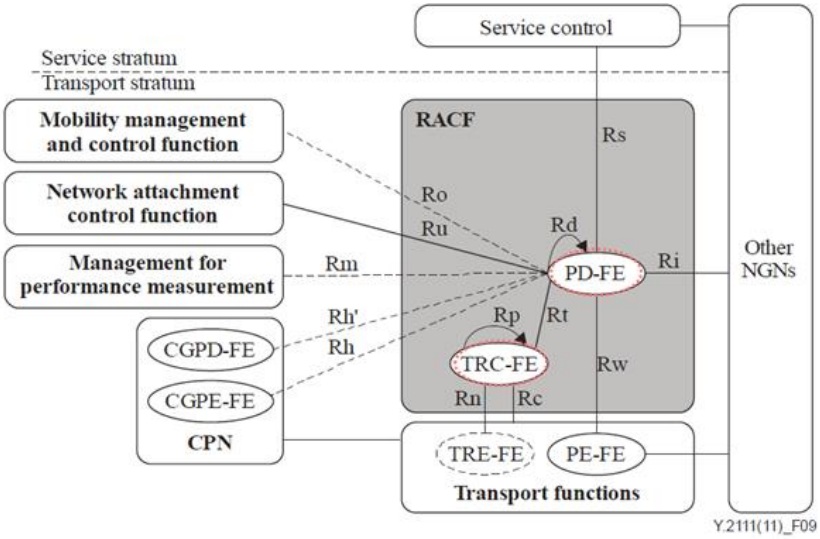

Figure 19: Y.2111, RACF main functional entities

Figure 19 shows the two reference points that constitutes prior art for the interface I2-S:

- Rh' RP: conveys information on QoS handling, priority handling and resource usage between PD-FE and the CGPD-FE (also inter-domain)
- Rh RP: allows PD-FE to push policy decisions to CGPE-FE, and CGPE-FE to request admission decisions (only intra-domain).

Y.2111 specifies the following QoS control procedure:

- SCF-requested QoS control procedures:
  - QoS resource reservation procedure
  - QoS resource reservation procedure for a nomadicity/wholesale scenario
  - Admission decision activation procedure
  - Admission decision de-activation procedure
  - QoS resource modification procedure
  - QoS resource release procedure
- CPE-requested QoS control procedures:
  - SCF-requested QoS initial authorization procedure
  - CPE-requested QoS resource reservation procedure triggered by PE-FE
  - SCF-requested QoS initial authorization procedure for nomadicity scenario
  - CPE-requested QoS resource reservation procedure triggered by the PE-FE for a nomadicity scenario
  - CPE-requested QoS resource modification procedure
  - Admission decision activation procedure
  - Admission decision de-activation procedure
  - CPE-requested QoS resource release procedure
  - SCF-requested QoS resource release procedure

Mainly there are three types of procedures:

- *QoS resource reservation*/modification/release procedures, which can be requested both by CPE (in pull mode, scenario 2) and SCF; they are meant to request a policy decision to the PD-FE and a final admission decision with consequent resource commitment at the PE-FE;
- *Admission decision activation*/deactivation procedures, which can be requested by the SCF: depending on the network policy rules and service requirement, either single-phase or two-phase resource commitment schemes are applied; in the single-phase scheme, the gates are opened and the requested resource is allocated immediately when the final admission decisions are installed in the PE-FE. In the two-phase scheme, the final admission decisions are installed in the PE-FE first; however, the admission decisions are not enforced until an admission decision activation is received from the SCF.
- *QoS initial authorization* procedures, which can be performed by the SCF: in pull mode, the SCF requests QoS initial authorization and then the CPE requests QoS resource reservation.

The main difference of the CONFIG framework from ITU-T NGN specifications is that End device and S-Plane have equal dignity, so that the Application requesting a session establishment (resource reservation in Y.2111) may reside the S-Plane and in the End device.

B.1.2 3GPP convergence related specifications

In the scope of CONFIG, the most relevant 3GPP prior art are the EPC architecture enhancements for non-3GPP accesses specified in TS 23.402 and their comparison with the overall 3GPP framework for what concern identity management, policy management and mobility management.

The most relevant sections of 3GPP TS 23.402 are:

- Section 4.7: IP Address Allocation over S5/S8, S2a (PMIPv6), S2b (GTP or PMIPv6), S2c;
- Section 4.8: Network Discovery and Selection (focusing on ANDSF);
- Section 4.9: Authentication (based on IETF protocols, e.g. EAP), making reference to TS 33.402 for the description of the procedures;
- Section 4.10: QoS Concepts, “the granularity of the QoS information that is passed over Gxa, Gxb and Gxc is the same as over Gx (on packet filters and associated QoS parameters (QCI, ARP, MBR, GBR))”;
- Section 5-7: functional descriptions and procedures;
- Section 8: handover procedures between 3GPP and non-3GPP accesses.

For what concern the core-access interface I3, Figure 20 provides an overview of the interfaces specified by TS 23.402:

- S2a provides UP with related control and mobility support from PGW to Trusted non 3GPP IP access;
  - S2a interface is based on IETF Proxy Mobile IPv6 (PMIPv6) S2a also supports (Client) Mobile
    - S2a may also be based on 3GPP GTP for Trusted WLAN,
    - IPv4 in case Trusted Non 3GPP IP accesses do not support GTP and PMIPv6
  - S2b interface is based on GTP or PMIPv6
- Gxa provides transfer of (QoS) policy information from (v)PCRF to Trusted Non-3GPP accesses;
- SWn is RP between Untrusted Non-3GPP IP Access and ePDG. Traffic on this interface for a UE-initiated tunnel has to be forced towards ePDG;
- SWa connects Un-trusted access points to the 3GPP AAA proxy;
- STa connects Trusted non-3GPP IP Access with 3GPP AAA Server/Proxy and securely transports access authentication, authorization, mobility parameters and charging-related information.

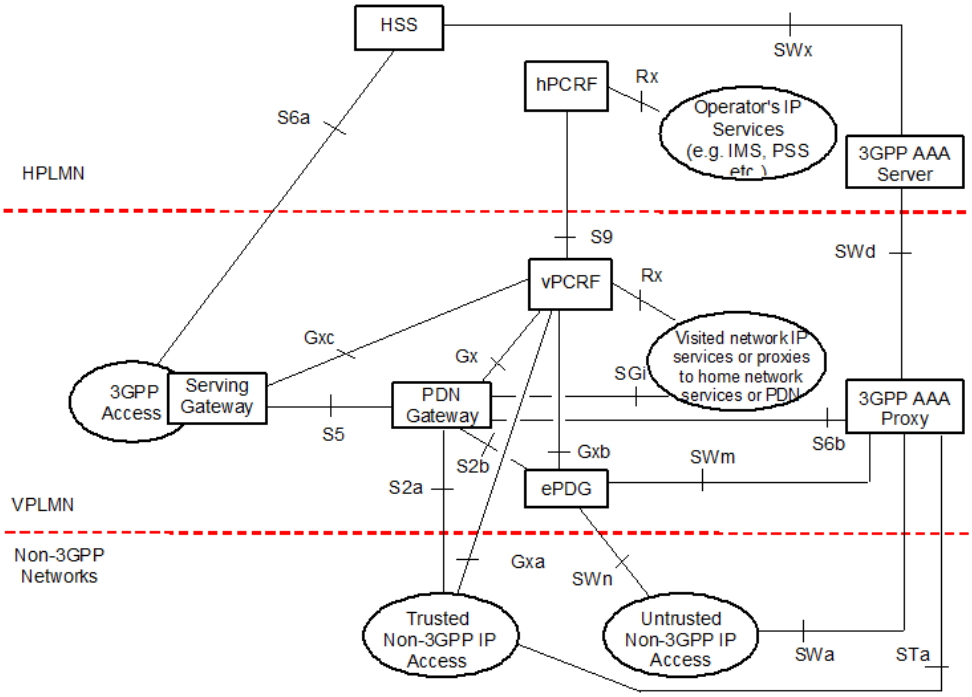

Figure 20: TS 23.402: EPS Roaming Architecture using S5, S2a, S2b (Local Breakout), Core–Access i/f

S1-MME and S1-U between 3GPP Access (RAN) and MME and SGW, respectively (not shown in the figure), are defined in TS 23.401. S5 can be based on GTP or PMIPv6.

For what concern the direct interface I2-C between UE and core, the interfaces S2c and SWu in TS 23.402 are important prior art (Figure 21).

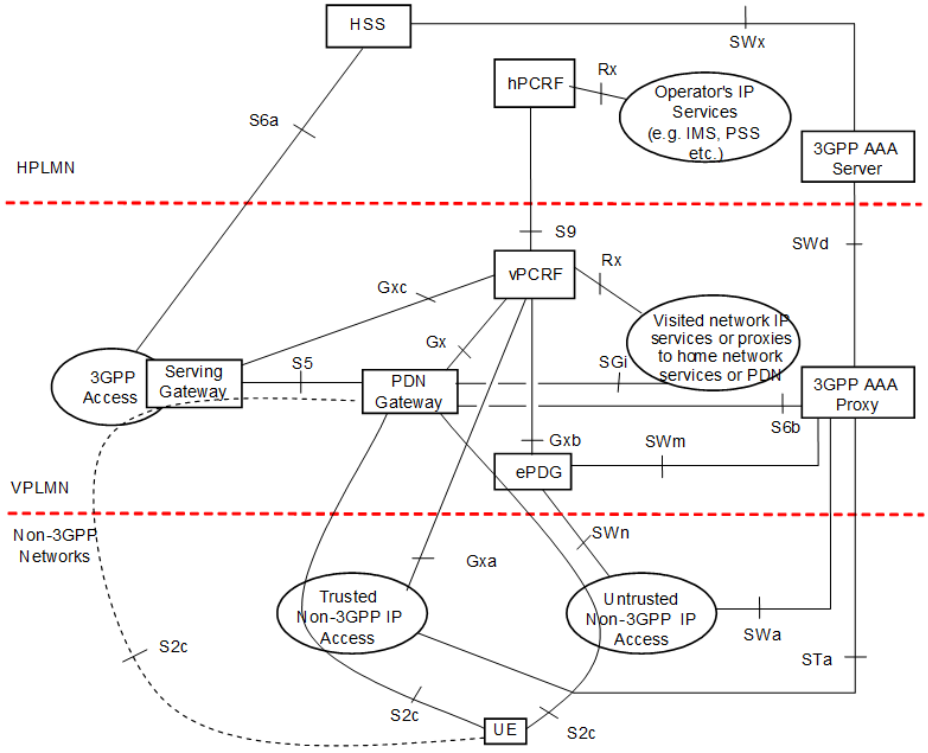

Figure 21: Roaming Architecture for EPS using S5, S2c – Local Breakout

- S2c provides UP with related control and mobility support between UE and PGW. This reference point is implemented over trusted and/or untrusted non-3GPP Access and/or 3GPP

access. S2c is based on DSMIPv6 (Dual Stack Mobile IPv6). NOTE: the implementation of this interface issues requirements to the UE.

- SWu is RP between UE and ePDG and supports handling of IPSec tunnels. SWu is based on IKEv2 (Internet Key Exchange Protocol Version 2) and MOBIKE (IKEv2 Mobility and Multihoming Protocol). Functionality of SWu includes
  - UE-initiated tunnel establishment and tear down
  - user data transmission within IPSec tunnel
  - support for IPSec tunnels fast update during HO between two untrusted non-3GPP IP accesses.

In conclusion, Figure 22 provides an overview of 3GPP interfaces that constitutes relevant prior art for the functionalities to be supported by WBI I3 (red lines) and I2-C (green lines).

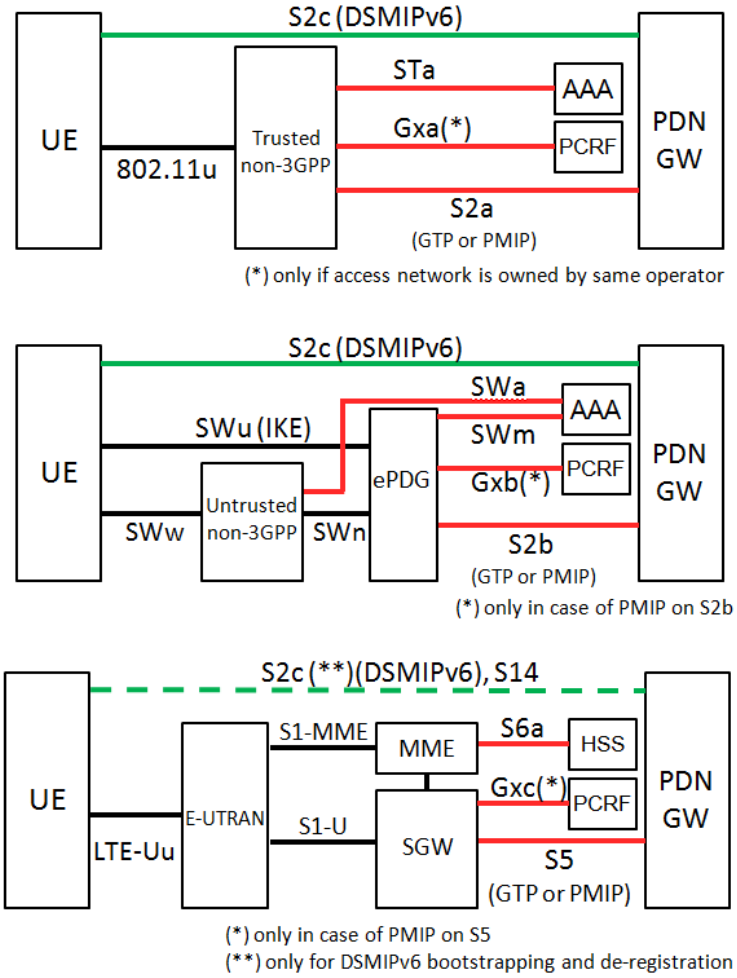

Figure 22: Overview of 3GPP prior art for interfaces I3 (red lines) and I2-C (green lines)

For what concerns the functionalities of S-GW, P-GW and ePDG, TS 23.402 assigns the following (see also Figure 23):

- S-GW:
  - MAG (Mobile Access Gateway) according to PMIPv6 specification, RFC 5213, if PMIP-based S5 or S8 is used
- P-GW:
  - LMA (Local Mobility Anchor) according to the PMIPv6 specification, RFC 5213, if PMIP-based S5 or S8, or if PMIP-based S2a or PMIP-based S2b is used
  - A DSMIPv6 Home Agent, as described in RFC 5555, if S2c is used

- ePDG:
  - MAG according to the PMIPv6 specification, RFC 5213, if PMIP based S2b is used
  - Allocation of a remote IP address as an IP address local to the ePDG which is used as CoA when S2c is used.

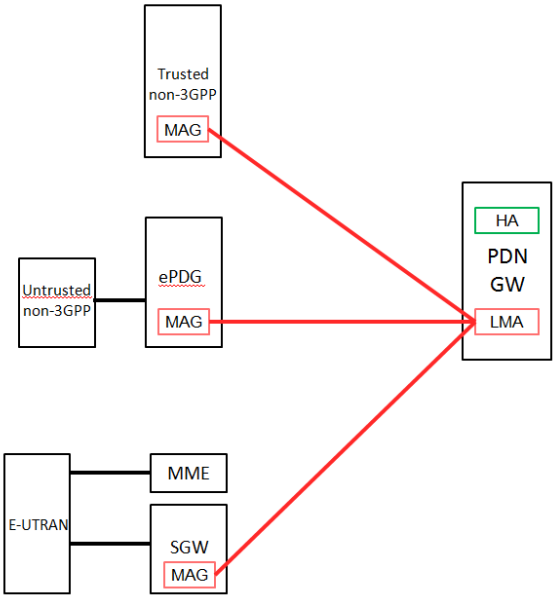

Figure 23: PMIP and DSMIP related functionalities in 3GPP TS 23.402

B.1.3 WiFi Alliance Passpoint and 3GPP ANDSF

Hotspot 2.0 Release 2 (2014) [22], which describes Network Selection and Security, and Online Signup and Policy Provisioning, specifies reference points between Hotspot functional elements and AAA and Policy Control functions in 3GPP core. It can be used as an input to identify relevant convergent core network functions, define access specific westbound interface and non access specific interface to the device.

Various interfaces defined for the interoperability between WiFi Hotspot and 3GPP networks are summarized in Figure 24.

For what concerns I3, the interfaces STa/SWa (already mentioned in Section B.1.3) are relevant prior art.

For interface I2-C, the 3GPP interface S14 (specified in [16]) is an important reference for what concern transferring network selection policies to the end device. S14 is an IP-based interface. The ANDSF client and server communicate using the OMA-DM protocol. There are two models of communication:

- Pull mode:
  - ANDSF Discovery by UE;
  - UE contacts ANDSF to request policy information;
  - UE interprets and acts on the policy.
- Push mode :
  - Policy is pushed to UE (SMS is the most common method);
  - The pushed message provides full information;
  - Alternatively, it may result in UE contacting ANDSF for more information (i.e. Push may be just a Pull trigger).

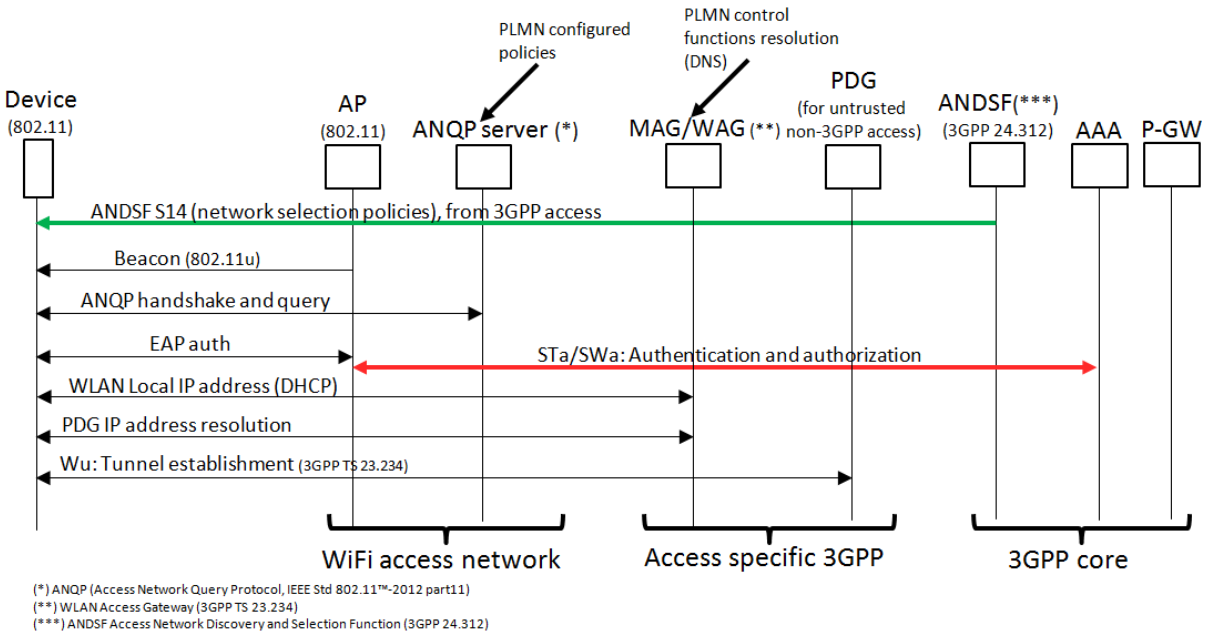

Figure 24: Interoperability between WiFi Hotspot and 3GPP network elements

B.1.4 IEEE OmniRAN TG

Reference between WBI_framework and OmniRAN related prior art for interface I2-C and I3 has not yet been discussed (see e.g.[19])

B.1.5 BBF

In BBF TR-101 [25] the Broadband Network Gateway (BNG) is an IP Edge Router where bandwidth and QoS policies may be applied. The term BNG is used instead of BRAS to denote an Ethernet-centric IP edge node in this document. The BNG provides Class of Service distinction and user isolation and traceability. The BNG terminates at least one PPP session (with PPPoE session identifier) per residential customer, monitoring its state using keep-alive messages and applying traffic profiles to it. According to [26], splitting PPPoE and PPP into the respective control and data planes would simplify the role of the BNG. Session establishment frames would be handled by a “controller”, leaving to the BNG the role of enforcing the QoS policies of the data plane.

TR-134 [27] defines an architectural Broadband Policy Control (BPC) Framework to provide policy control of Broadband Multi-Service Networks. A large number of high level business requirements for policy have been captured in existing Broadband Forum documents, in particular TR-058, TR-059, TR-092, TR-101, TR-102, TR-144 and TR-147. TR-134 re-affirms existing requirements and introduces new ones for what concern:

- Session management: BPC framework must support
  - policies associated with access, L2, subscribed and application session types
  - interaction with session establishment
  - policy change request from applications after session establishment
- Application Admission control:
  - The BPC Framework enables applications to participate in the allocation of network resources through signalling.
  - The BPC Framework enables the operator to control the acceptance of application traffic into the network based on policy rules. The decision criteria that lead to an admission control decision may include both network and business rules.
- QoS and bandwidth management: The BPC Framework enables policies
  - to control the allocation of bandwidth resources in the access network

- to allocate traffic flows to QoS classes in the access network.

AAA: The BPC Framework must support the exchange of RADIUS and Diameter accounting messages with the AAA Server or network elements like the BNG.

The BPC Architecture is shown in Figure 25. The name of the entities (PDP: Policy Decision Points, PEP: Policy Enforcement Points) refers to ITU-T NGN entities in the RACF framework [20]. Explicit mapping is done in TR-134 Appendix II.

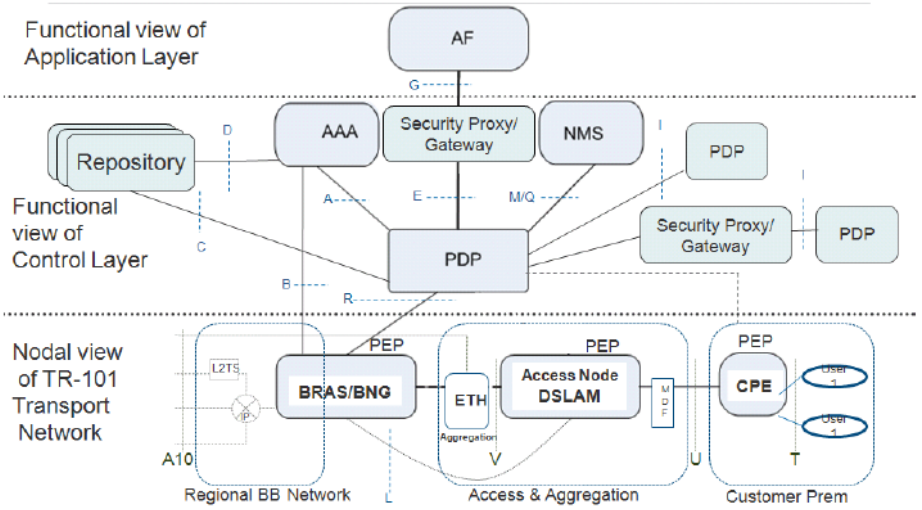

Figure 25: BPC Framework Interface Architecture mapped into TR-101 architecture

The upper layer in the figure, the AF, corresponds to the S-Plane in the CONFIG framework. The medial part, the control layer, corresponds to the C-Plane of CONFIG. The BPC Framework envisages architectures in which the PDP functionality can be centralized or distributed in various physical and nodal locations.

BBF TR-134 specifies the following sets of information exchanges:

- AF -> PDP: Information on the incoming call/session from the BBF domain AF is conveyed to the PDP;
- AAA -> PDP: Information on the authorization and authentication status is conveyed to the PDP.
- PDP -> PEP: The PDP processes all incoming information and submits it to the PEP;
- PEP -> PDP: The PEP submits the policy enforcement status back to the PDP or PEP requests policy decision from the PDP;
- PDP -> AF: The PDP responds back to the AF with information on acceptance or rejection of the incoming call/session.
- PDP -> PDP: The PDP receives information from another PDP.
- PDP -> PDP: The PDP sends information to another PDP.

We can map each BBF TR-134 information exchange to the CONFIG interfaces as follows:

Table 3: Mapping between BBF info exchange and CONFIG interfaces

#	BBF info exchange	CONFIG interface
1.	AF->PDP	I2-S (NBI)
2.	AAA->PDP	Internal C-Plane interface
3.	PDP->PEP	I3

4.	PEP->PDP	I3
5.	PDP->AF	I2-S (NBI)
6.	PDP->PDP	East Bound Interface
7.	PDP->PDP	East Bound Interface

References

[1] https://www.5g-ppp.eu/

[2] METIS Deliverable D1.1 ”Scenarios, requirements and KPIs for 5G mobile and wireless system”, ICT-317669-METIS/D1.1, March 2013

[3] 3GPP, “Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14), v0.1.0 ,” tech. rep

[4] 3GPP TS 23.401, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access,” Release 12.

[5] 3GPP TS 23.203, “Policy & charging control architecture,” Release 12.

[6] 3GPP TR 36.912, “Feasibility study for Further Advancements for E-UTRA (LTE-Advanced),” Release 12.

[7] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses

[8] 3GPP TS 23.161, Network-based IP flow mobility and Wireless Local Area Network (WLAN) offload

[9] IEEE 802.1CF, Network Refernce Model and Functional Description of IEEE 802 Access Network, http://www.ieee802.org/1/pages/802.1cf.html

[10] 5G NORMA, 5G Novel Radio Multiservice adaptive network Architecture, https://5gnorma.5g-ppp.eu/

[11] A.K.D Dey, G.D. Abowd, Towards a better understanding of context and context awareness, Workshop on The What, Who, Where, When, and How of Context Awareness, affiliated with the 2000 ACM Conference on Human Factors in Computer Systems (CHI 2000), The Hague, Netherlands, April 2000.

[12] T. Schmidt, M. Wählisch, and S. Krishnan, "Base Deployment for Multicast Listener Supphort in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011, online available at https://tools.ietf.org/html/rfc6224

[13] T. Schmidt, S. Gao, H. Zhang, M. Wählisch, “Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains”, RFC 7287, June 2014, online available at https://tools.ietf.org/html/rfc7287

[14] Recommendation ITU-T Y.2018, “Mobility management and control framework and architecture within the NGN transport stratum”, ITU-T, Geneve, 2009

[15] 3GPP TS23.402 Rel.13, “Architecture enhancements for non-3GPP accesses“

[16] 3GPP TS24.312 “Access Network Discovery and Selection Function (ANDSF) Management Object (MO)”

[17] H. Soliman et al., “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)”, IETF RFC 5555, June 2009

[18] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6”, IETF RFC 5213, 2008

[19] IEEE 802.1CF OmniRAN, Draft Recommended Practice for Network Reference Model and Functional Description of IEEE 802 Access Network, work in progress, 2015, see e.g. http://www.ieee1904.org/2/meeting_archive/2015/02/tf2_1502_elbakoury_3.pdf and/or https://mentor.ieee.org/omniran/dcn/15/omniran-15-0035-02-CF00-cf-text-review.pdf

[20] ITU-T NGN, Y.2111 - SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL

ASPECTS AND NEXT-GENERATION NETWORKS Next Generation Networks – Frameworks and functional architecture models - Resource and admission control functions in next generation networks

[21] Y.2012 - SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS Next Generation Networks – Frameworks and functional architecture models

[22] Wi-Fi Alliance Hotspot 2.0 (Release 2) Technical Specification - Version 1.1.0, 2015

[23] Wi-Fi CERTIFIED Passpoint™ (Release 2) Deployment Guidelines Rev 1.0 , October 8, 2014

[24] ANDSF Access Network Discovery and Selection Function (3GPP 24.312, v13.1.0, Nov 2015)

[25] BBF TR-101 Migration to Ethernet-Based DSL Aggregation, Issue 2, July 2011

[26] Woesner, H.; Fritzsche, D., "SDN and OpenFlow for converged access/aggregation networks," Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), 2013 , vol., no., pp.1,3, 17-21 March 2013

[27] BBF TR-134: Broadband Policy Control Framework (BPCF), Issue: 1, Corrigendum 1, January 2013

[28] NGMN Alliance, 5G White Paper, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

[29] CONFIG Del. 1.2

[30] H. J. Einsiedler, R. L. Aguiar, A. Gavras, and H. D. Schotten, "A new metamodel for Future Internet architectures", Future Network & Mobile Summit 2013, 3-5 July 2013, Lisbon, Portugal, Conference Proceeding, ISBN: 978-1-905824-36-6, IEEE published (see http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6633521)

