Paper number ITS-XXXX

5G network considerations for CCAM functionality support in roaming / cross-border conditions

Konstantinos Trichias[1*], Nazli Guney[2,3], Erdal Berbel[2], Foteini Setaki[4], Pedro J. Fernandez[5]

1. WINGS ICT Solutions, Greece, ktrichias@wings-ict-solutions.eu

2. Turkcell, Turkey, {nazli.guney, erdal.berber}@turkcell.com.tr

3. Istanbul Rumeli University, Turkey, nazli.guney@rumeli.edu.tr

4. Cosmote, Greece, fsetaki@cosmote.gr

5. University of Murcia, Spain, pedroj@um.es

Abstract

Despite the proven added value of 5G connectivity for advanced Cooperative, Connected and Automated Mobility (CCAM) showcased via recent trials with the use of autonomous vehicles in experimental 5G networks, the technical and business aspects of supporting advanced CCAM scenarios in realistic cross-border conditions has not been thoroughly investigated yet. The stringent requirements of cutting-edge CCAM applications need to be met during roaming between neighbouring 5G networks, while continuous service provisioning and retainability of the Quality of Service (QoS) should be guaranteed. In this paper, we address the main architectural considerations regarding the deployment of 5G networks capable of supporting CCAM functionality at cross-border conditions, as formulated by major European Mobile Network Operators (MNOs). This work, which is part of the H2020 5G-MOBIX project [1], touches upon 5G inter-Public Land Mobile Network (PLMN) and inter-Multi-Access Edge Computing (MEC) interconnection, functional and non-functional requirements, as well as security and privacy considerations.

Keywords: 5G-ROAMING, CROSS-BORDER CCAM, INTER-PLMN HO

Introduction

As per the European Union long term vision, the Trans-European Transport Network (TEN-T) initiative [2] defines nine critical corridors for transportation across Europe where advanced CCAM services are expected to be fully supported by 2025, mainly enabled by 5G connectivity. Even though the suitability of 5G networks for CCAM deployment in urban and highway conditions have been well studied and even demonstrated through real-life trials (e.g. [3]), the operation in the challenging cross-border conditions necessary to realize the vision of Pan-European corridors, has barely been addressed. Moreover, as most trials so far have been performed in controlled environments (e.g. specialized tracks, etc.) using test networks, real-life network roll-out, integration and interconnection aspects have not been considered either, which are critical for the engagement of important stakeholders and the generation of solid deployment roadmaps. Finally, the impact on CCAM application performance of early releases of 5G networks (e.g. 3GPP Rel.15) using Non-Stand Alone (NSA) architecture (3GPP option 3x), has not been investigated even though these types of architectures will dominate the European landscape, until more mature releases become available.

In an attempt to address these challenges and to enable the EU vision, the H2020 5G-MOBIX project [1] aims to qualify 5G as a core connectivity infrastructure that can address a broad set of CCAM V2X use cases in *cross-border conditions*, having a business appeal for a sufficiently large number of stakeholders to justify the investments required to deliver 5G mobility services in the near future, especially at currently underserved cross-border areas. With the contribution of major European vendors, MNOs, Original Equipment Manufacturers (OEMs) and technology developers the project will set-up two cross-border corridors utilizing neighbouring MNOs' 5G-NSA networks (with potential upgrade to SA) to provide connectivity and support for advanced CCAM use cases, while roaming among European countries.

This paper provides an overview of the work of the 5G-MOBIX network experts (for details see [4]), as they attempt to address the issues that arise from provisioning CCAM services in cross-border conditions over real-life 5G NSA networks, such as End-to-End (E2E) latency minimization, service continuity, connection re-establishment, inter-MEC connectivity, inter-PLMN Hand Over (HO) and security/privacy concerns. In more detail, the following aspects are addressed: i) overview of roaming standardisation support including inter-PLMN and inter-MEC connectivity, ii) functional and non-functional requirements for cross-border operation, iii) security and privacy considerations for cross-border operation and iv) basic 5G architecture design for cross-border operation.

Roaming Support for Advanced CCAM functionality

The 5G-enabled CCAM use cases envisioned by the 3GPP and detailed in [5] are much more advanced and demanding than the early-phase safety/efficiency applications envisioned for cooperative-intelligent transport systems (C-ITS). As the automotive industry turns its attention towards more data-hungry applications including for instance raw sensor data exchange, coordination of future manoeuvre, video streaming and more, which need to be transmitted with stringent requirements regarding data-rate, latency, reliability, range, speed and more [5], the enhanced communication capabilities of 5G mobile networks will be required for proper service provisioning.

For network operators to be able to support these advanced Vehicle-to-Everything (V2X) applications across European corridors, international roaming support is important to ensure that CCAM functionality can be seamlessly executed while the vehicles traverse from one country to the other and get serviced from different MNOs. The trade-off between end-to-end (E2E) latency while roaming versus service continuity during inter-operator handover stands out as one of the biggest obstacles for design, deployment and commercialization of delay-sensitive services when roaming to another MNO. However, current roaming agreements among operators for commercial services can only support basic communication flows without any kind of QoS guarantees for stringent services and are thus unable to support advanced CCAM use cases during roaming.

Roaming support in Standardisation

For the 5G-NSA deployment option (EPC acting as the core network) inter-operator roaming requires that at least one of the two 3GPP roaming standards of Home Routed (HR) and Local Break-Out (LBO) as well as the necessary roaming interfaces are supported by the MNOs [6]. The two options are defined based on the Packet Data Network Gateway (PDN-GW) that serves the roaming user.

- **Home Routed (HR):** Subscribers always obtain service from the home PDN gateway (H-PGW) and through their home network, resulting in inherent service continuity while roaming, but with increased latency and resources/bandwidth utilisation due to the user plane traffic being routed to the Home PLMN.
- **Local Break-Out (LBO):** Subscribers obtain service from the visited PGW (V-PGW) resulting in significantly reduced roaming service delay (payload traffic does not traverse back to the H-PGW, but rather stays in the V-PLMN network), at the expense of service control, policy control, charging and service continuity that will be disrupted as the sessions must be released and re-established during the handover. LBO, which is a spec-compliant functionality, requires re-establishment of PDN session.

In 5G-SA deployments, the Session and Service Continuity (SSC) mode determines the roaming policy. With SSC mode 3, the network ensures that a UE does not lose connectivity by making a new connection before breaking the existing one to allow for service continuity making it the most promising option for the support of advanced CCAM applications. This option however is only feasible between two 5G-SA networks, while 5G-NSA HO and hybrid SA-NSA HO still suffer from the inadequacies of HR or LBO based roaming.

Inter-PLMN connectivity

Currently two MNOs may interconnect their networks either over the GRX / IPX network or via a direct connection. The pros and cons of each solution for CCAM functionality support are discussed in this sub-section.

- **Direct Interconnection** is simple and if established through private lines or VPNs (ex. MPLS) can solve QoS and security issues. Nevertheless, it greatly increases cost especially if many international point-to-point private lines are necessary, as is the case for CCAM functionality support across pan-European corridors spanning multiple countries (and MNO domains). Hence this solution suffers from inherent scalability issues.
- **GRX based Interconnections** are point-to-multi-point connections operated and managed by third parties. Each MNO can be connected to multiple operator networks through a GRX connection endpoint establishing corresponding roaming agreements. This solution greatly reduces roaming costs and is highly scalable, but no QoS can be guaranteed for any type of service making it highly unsuitable for CCAM applications, where certain requirements need to be met at all times.
- **IP exchange (IPX) based Interconnections** are an evolution of the GRX framework assuming an all-IP transformation better suited for LTE service requirements. IPX networks can offer

certain E2E Service Level Agreements (SLA) by utilizing the Diameter Edge Agent (DEA) [7], which is considered as the only point of contact into and out of an operator's network and has been widely used in the S6a, S6d, S9, S13, Gx, Gxc, and Rx interfaces of the 3GPP EPC architecture. Nevertheless, advanced CCAM applications requiring 5G level performance in terms of latency and reliability could not be provisioned over IPX interconnections.

Inter-MEC connectivity and mobility support

For the proper provisioning of CCAM functionality while roaming, the type of MEC deployed as well as their interconnection among neighbouring MNOs also plays a major role. For the 5G NSA architecture where a 4G core and interfaces are used, a fallback into 4G MEC deployment options is necessary. The resulting MEC deployment options as well as interconnection possibilities to support user mobility are summarised below:

- **Bump in the Wire:** In this scenario, to support low latency communications, the MEC host is placed on the S1 interface of the system architecture in between the eNB/gNB and the core network components (SGW, PGW, MME etc), and the MEC host's data plane must process user traffic encapsulated in GPRS Tunnelling Protocol – User plane (GTP-U) packets. This scenario poses challenges to operations such as lawful interception and charging, possibly mandating a dedicated solution such as a MEC GW to be implemented.
- **Distributed EPC:** In this scenario, through its data plane the MEC host is placed on the SGi interface, connected to the distributed EPC components, where the Home Subscriber Server (HSS) is co-located with the EPC, and the MEC applications can also be positioned next to the EPC functions in the same MEC host. The advantage of the distributed EPC scenario is that it requires less changes to the operator's network and leverages standard 3GPP entities for session management and charging operations.
- **Distributed S/PGW:** This scenario is similar to the Distributed EPC except that only SGW and PGW entities are deployed at the edge site, whereas the control plane functions such as the Mobility Management Entity (MME) and HSS are located at the operator's core site.
- **Distributed SGW with Local Breakout (SGW-LBO):** Local breakout of the MEC data at the SGWs to achieve a greater control on the granularity of the traffic that needs to be steered such as to allow the users to reach both the MEC applications and the operator's core site application in a selective manner over the same access point name (APN).
- **CUPS MEC:** The deployment options above with distributed EPC gateways at the edge, can also be built using the Control and User Plane Separation (CUPS) paradigm standardized in 3GPP Rel.14 and have the new User Plane built in the MEC host allowing the traffic to be locally steered.

As mobility management affects the service continuity it is considered especially critical for CCAM applications, and since MEC functionality is an inherent part of most advanced CCAM application, **inter-MEC mobility / HO** is equally critical to meet the necessary requirements. In order to provide service continuity to a roaming UE, the MEC system needs to relocate the service delivered to the UE from the source to the target MEC. In the distributed EPC, distributed S/PGW, SGW-LBO and CUPS MEC deployment options, the MEC handover is supported using 3GPP standard "*S1 Handover with SGW relocation*" by maintaining the original PGW as anchor (HR option). Nevertheless, it is the MEC application's responsibility to synchronize at application level and maintain the session in the case of a stateful application. Such a solution suffers from the inherent issues of the HR option discussed above and cannot support demanding CCAM application. In cases of direct network interconnection, the available MECs may also utilize this connection inheriting however both the increased performance and scalability concerns.

Functional and Non-Functional Requirements for Cross-Border Operation

In order to properly set-up and configure the RAN and core parts of the 5G network to support CCAM functionality at cross-border conditions, the main functional and non-functional requirements of such a system need to be identified. The *functional requirement*s practically specify "what a system should do", i.e. the behaviour of the system when certain conditions are met, while the non-functional requirements specify "how the system performs certain functions", i.e. the expected behaviour of a system and the limits of its functionality. 5G network experts from the 5G-MOBIX project [1], comprising five major European MNOs, two major European vendors and other experts, have identified and prioritised the most prominent functional and non-functional requirements 5G networks should fulfil in order to support CCAM functionality in cross-border conditions.

These requirements range from the support of specific functionalities in the radio, core and transport parts of the network down to SLA and roaming agreements. The prioritisation of each of the functional and non-functional requirements is based on the MoSCoW method of requirements prioritization [8], which is a well-established management method, prioritising the requirements of any system into (M)ust-haves (highest priority), (S)hould-haves, (C)ould-haves and (W)ould-haves (lowest priority). By assigning a numerical value to the MoSCoW grades (M=2, S=1, C/W=0), and by aggregating the responses of the experts around Europe (see [4] for exact details) a clear requirements prioritisation was established on a scale of one to ten (1 (low priority) – 10 (high priority)). The resulting classification per functional requirement is shown in Figure 1, while the classification of the non-functional ones is depicted in Figure 2.

Based on the above analysis the support for core eMBB functionality and the support for virtualization are the most critical functional requirements for delivering high quality CCAM services in cross border conditions. Both these features should become available with the deployment of 5G core solutions (i.e. SA implementations). Closely behind, mobility support and URLLC functionality will allow for further CCAM applications to be supported. In terms of non-functional requirements there does not seem to be a clear winner, as multiple requirements are deemed critical for the successful provisioning of CCAM services by 5G networks. Scalability, upgradability, physical and cyber-security, commercial feasibility and reliability are considered key factors that must be present for 5G networks to be able to realistically extend their functionality and reach to a state where they would successfully support the stringent CCAM applications.

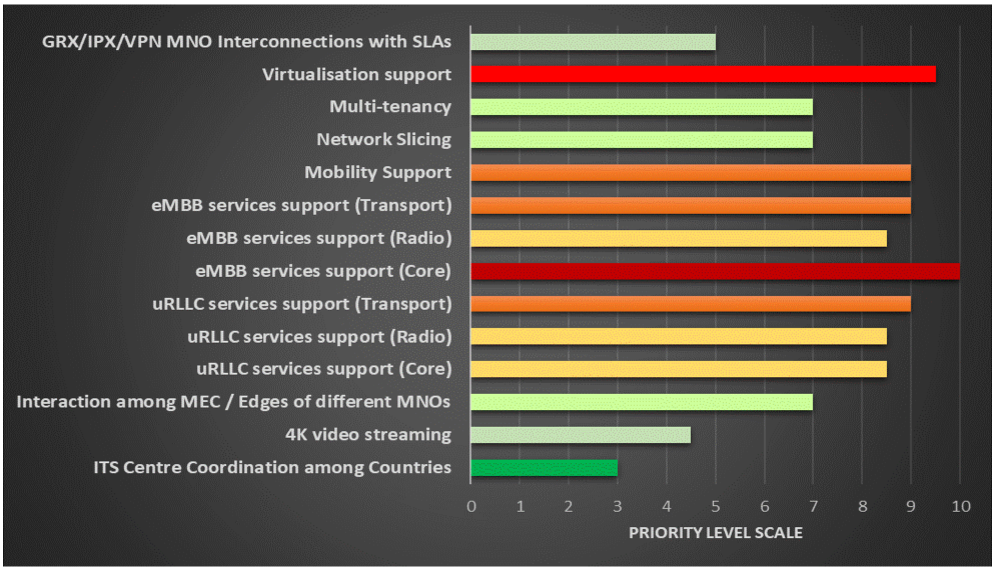

Figure 1 – Prioritisation of functional requirements for support of CCAM functionality

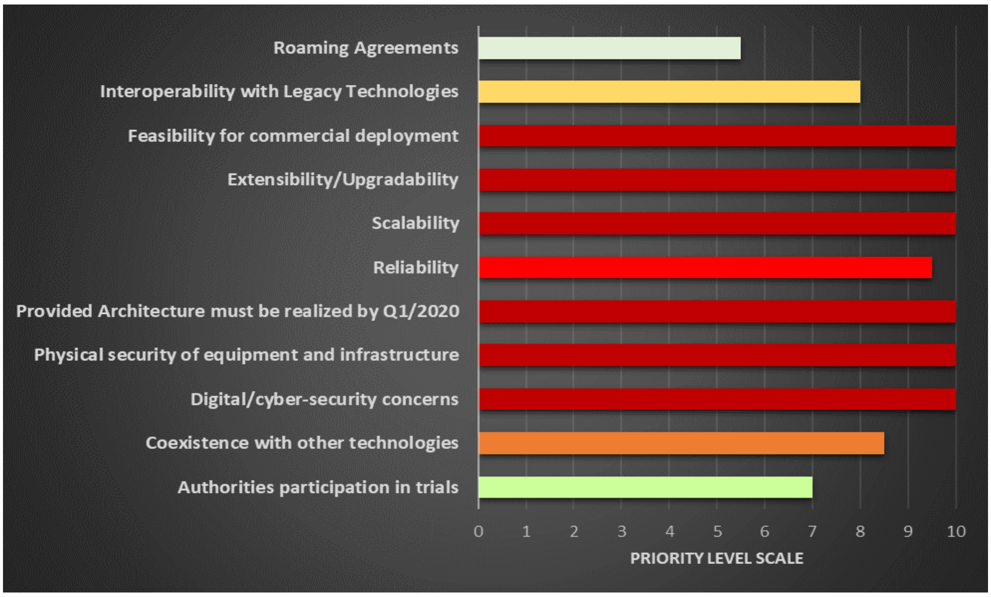

Figure 2 - Prioritisation of non-functional requirements for support of CCAM functionality

Security & Data Privacy Considerations for Cross-Border CCAM Support

The exploitation of the potential security vulnerabilities inherent to the various sub-systems comprising modern telecommunication networks could lead to massive disruptions. These issues must be properly and proactively addressed, especially in CCAM environments where human lives are at stake. Cross-border operation complicates things even further as it entails HOs between network operators that belong to different countries, raising several security and privacy concerns. The most representative ones are highlighted below.

- **Interoperation of different Trust Domains**: For the C-ITS messaging, an asymmetric cryptography method is applied to protect Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM) and provide data integrity, non-repudiation and other interesting security attributes. This implies the usage of Public Key Infrastructures (PKI) to issue certificates. EU countries use the same PKI infrastructure (European C-ITS Credential Management System), hence avoiding trust issues in EU internal borders. In EU external borders however, the vehicles connected to the respective MNOs may not trust each other (absence of common PKI) and ignore the content of C-ITS messages. As a result, the respective vehicle groups would be invisible to each other, which could result in application malfunction or even accidents.

- **Application of different Data Privacy Protection laws**: The European General Data Protection Regulation (GDPR)) directs the protection of CAM and DEMN messages, as they are also considered personal data due to sensitive information like the vehicle identification number that could be used by unauthorised parties. This issue becomes increasingly complex to handle in the external EU border where GDPR is not enforceable. Solutions like identity pseudonymization could significatively strengthen the user protection against traceability and should be part of any cross-border deployment.

Apart from these representative cross-border issues, MNOs have to consider even more specific security requirements that should be enforced, not only in border areas, but in all network deployments, to safely support CCAM functionality. A detailed analysis can be found in [4].

Cross-Border Architectural Considerations for 5G NSA deployments

While a significant portion of the previously discussed aspects will be addressed by default once 5G-SA network deployments are ubiquitously available, meeting these requirements during roaming operations over 5G-NSA networks (or 5G-SA to a 5G-NSA) is not as straightforward. Considering current vendor roadmaps regarding the availability of 5G core and the inherent latency until market adoption, the largest portion of the path towards 5G coverage over the main European corridors by 2025 (EC vision), will be dominated by NSA or hybrid solutions. Hence, it becomes critically important to ensure that roaming over 5G-NSA networks does not significantly degrade the network performance and is capable of providing the required QoS for advanced CCAM applications at the borders among European states. To this end, the architectural design regarding the inter-PLMN and inter-MEC connectivity of neighbouring 5G networks becomes critical, to ensure service continuity and / or reduced latency during inter-PLMN HO when supporting CCAM applications.

In the 5G-MOBIX project, three deployment and interconnection options were considered all with their own advantages and disadvantages, as discussed below. For each one of them the commercial components, the necessary overlay components as well as optional components are indicated in order to provide a better understanding of the deployment integration effort required.

- **Option 1 - Full GRX interconnection:** The first deployment option for the interconnection of the neighbouring MNOs is the traditional GRX interconnection. The two networks are interconnected using the S6a interface to connect the MME of the V-PLMN to the Home Subscriber Server (HSS) of the H-PLMN, the S8 interface for signalling and data transfer between Serving Gateway / Packet Gateway (SGW/PGW) entities and the S10 interface to exchange context information between the two MMEs. In a HR scenario, service continuity would be achieved, however significant latency would be observed on the application layer. The LBO solution might be more appropriate for CCAM applications in roaming scenarios as the roaming latency would be significantly reduced at the expense however of service control, policy control, charging and service continuity that will be disrupted as the sessions must be released and re-established during HO. Figure 3 depicts the network components (commercial and overlay) and their respective interconnections for deployment option 1.

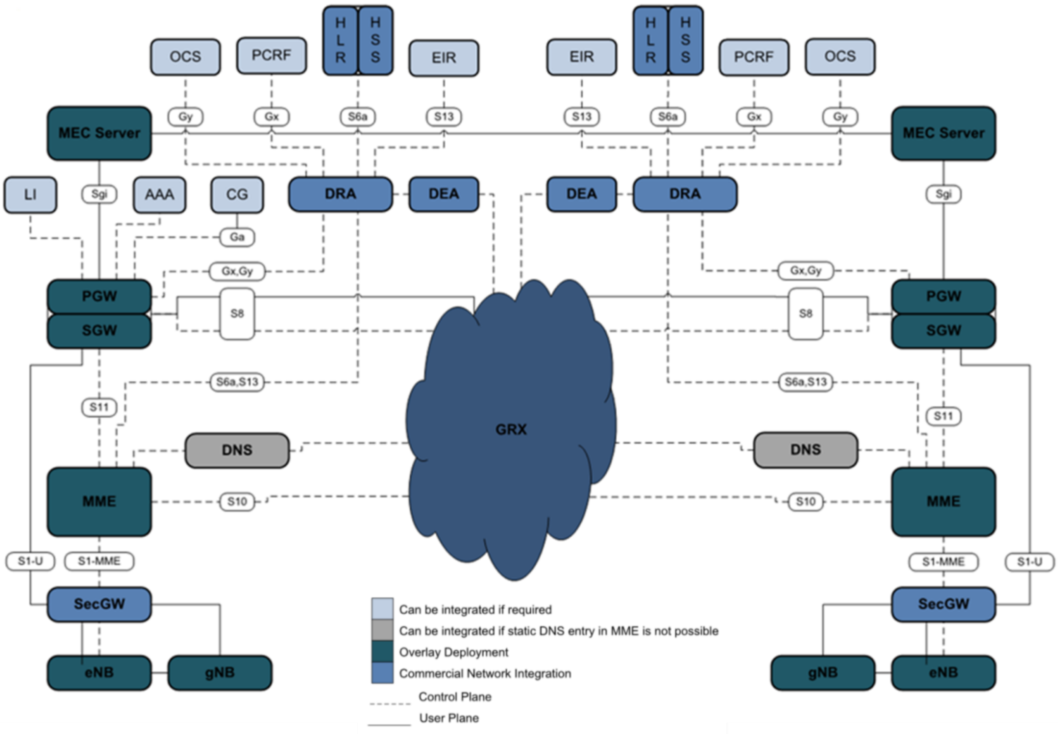

Figure 3 - Option 1: Full GRX interconnection

- **Option 2 - GRX interconnection for CP traffic & Direct interconnection for UP traffic:** The second deployment option is a mixed approach where all User Plane (UP) traffic is carried via a direct interconnection established between the neighbouring MNOs, while signalling / Control Plane (CP) traffic is still carried through the GRX network. This approach can significantly reduce the experienced latency for the user plane data (CCAM application data in this case) even without an LBO function, but an overlay direct interconnection will still have to be established between the two networks, adding to the complexity and introducing scalability issues. The network interconnection for option 2 is depicted in Figure 4.
- **Option 3 - Direct interconnection:** The third deployment option is based on an overlay dedicated network providing direct interconnection for both UP and CP traffic. As a result, significantly reduced latencies during roaming will be experienced by both the UP and CP traffic, allowing for the provision of service during roaming even to the more demanding CCAM applications. This options still suffers from increased complexity and scalability issues. Figure 5 depicts the interconnection of the necessary components for the implementation of option 3.

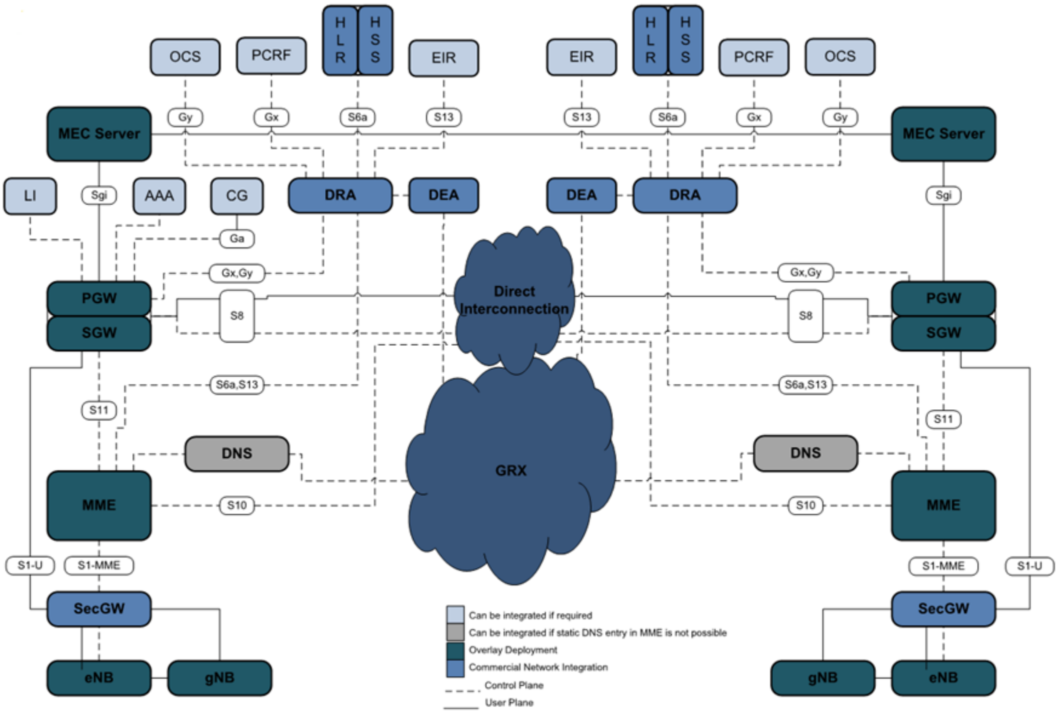

Figure 4 - Option 2: GRX interconnection for CP traffic & Direct interconnection for UP traffic

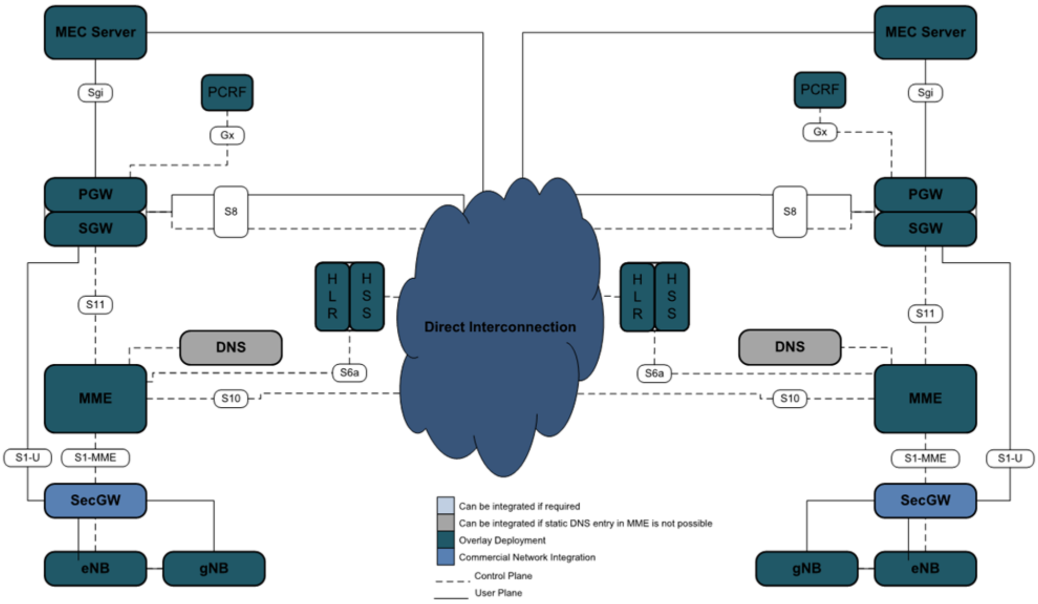

Figure 5 - Option 3: Direct interconnection

Among the three investigated options, option 1 is the most realistic for wide deployment across Europe, as it is readily available for most European MNOs (to some extent), however it is almost certain that the most demanding CCAM applications will not be supported during roaming. In order to guarantee the needed QoS by CCAM applications, deployment option 3 is the most suitable as it offers both service continuity and low latency during roaming. Even though a Europe wide direct interconnection of MNOs is not realistic, national roaming plans, the gradual introduction of 5G core features and spatio-temporal planning of network resources may mitigate the scalability concerns raised by option 3. As part of the 5G-MOBIX trials, option 3 will be considered as the main deployment option for cross-border trials over 5G-NSA networks, as it is expected to be the only one capable of supporting the demanding 5G-MOBIX CCAM applications during roaming.

Conclusions

This paper investigates the 5G network aspects that need to be considered for 5G-NSA networks deployed in cross-border areas to be capable of supporting the demanding CCAM applications. The currently supported roaming and mobility functions have been analysed, various inter-PLMN and MEC deployment and interconnection options have been considered while a prioritization of the main requirements to support CCAM cross-border functionality according to major European MNOs and vendors, and the main security and privacy concerns, have also been presented. Based on this analysis, a basic architectural design has been selected for the 5G networks that will be deployed between Spain-Portugal and Greece-Turkey, where real-life advanced CCAM trials will take place from May 2020 onwards, to showcase the suitability of 5G-NSA for cross-border CCAM operations [1].

Acknowledgements

This work is a part of the 5G-MOBIX project. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 825496. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

References

1. H2020-ICT-18-2018 5G-MOBIX project “5G for cooperative & connected automated MOBIility on X-border corridors”, Nov. 2018 – Nov.2021, https://www.5g-mobix.com/
2. Trans-European Transport Network (TEN-T) core corridors: http://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/map/maps.html
3. AUTOPILOT project - Large-Scale Pilots (LSPs) on the Internet of Things: Pilot 5: autonomous vehicle in a connected environment, https://autopilot-project.eu/
4. 5G-MOBIX deliverable D2.2, “5G architecture and technologies for CCAM specifications”, 31st October, 2019, https://www.5g-mobix.com/hub/deliverables
5. 3G PP TR 22.886, “Study on enhancement of 3GPP Support for 5G V2X Services (Release 16)”
6. 3GPP TS 23.401, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 16)”.
7. LTE Roaming Guidelines: https://www.gsma.com/newsroom/wp-content/uploads/2013/04/IR.88-v9.0.pdf
8. MoScoW method explained, ToolsHero, https://www.toolshero.com/project-management/moscow-method/