Dynamic Authorization for 5G Systems

Samir Ferdi[2], Yogendra Shah[1], Vinod Kumar Choyi[1], Alec Brusilovsky[1]
[1]InterDigital Communications, Inc., Conshohocken, PA
[2] InterDigital Canada Ltee, Montreal, Canada
{samir.ferdi, yogendra.shah, vinod.choyi, alec.brusilovsky}@interdigital.com

***Abstract* — 5G Networks are being designed to provide a diverse set of services using Network Slices (NS) that are enabled by Network Function Virtualization (NFV) and Software Defined Network (SDN) technologies. Given the expected diversity of service offerings and variety of connected devices, it's desirable to have a service authorization architecture that accommodates delivery of services from a variety of infrastructure service providers, while simultaneously protecting these infrastructure service providers from unauthorized service consumption. We illustrate an authorization framework to enable dynamic, context-based authorization for services offered over 5G networks.**

Keywords—5G systems; access tokens; context-sensitive access control; dynamic authorization; NFV, network slice; OAuth; SDN, service negotiation; service selection; subscription profile; virtualized networks.

I. INTRODUCTION

The goal of 5G systems standardization is to not only meet an increased demand for traffic growth, but to also accommodate a diversity of service level requirements. The use cases driving the 5G network architecture vary from an ongoing need for Enhanced Mobile Broadband (eMBB) connectivity, Massive Internet of Things (MIoT) to Ultra-Reliable Low Latency Critical Communications (URLLC) services [1]. In addition, 5G systems will need to interwork with the previous generation Evolved Packet System (EPS).

Collectively, the flexibility of delivering services using a NS architecture aligns well with the desire to offer a rich set of application layer services to 5G system subscribers, while taking into consideration architectural approaches for the deployment of 5G networks that reduce CAPEX and OPEX costs.

Legacy wireless networks have provided a complete set of application services within a single network. Authentication and implicit authorization provide access to a full spectrum of services offered by the network. However, with 5G networks and NSs, the services may be provided over one or more NSs, which may be operated by multiple infrastructure service providers/stakeholders. Furthermore, it is desirable to provide access authentication and subsequent authorization to only those services that are aligned with the UE subscription, rather than full access to the multiplicity of services across multiple NSs. Hence, the motivation to provide a dynamic, context sensitive authorization mechanism that provides granular access to services of a 5G network, as applications are accessed by a UE.

This paper is organized as follows. Section II provides a background to authorization requirements, and prior work pertaining to 5G systems. Section III provides an overview of an authorization framework that evolves from current 4G systems to accommodate dynamic service negotiation in 5G. Section IV provides illustrative technical details of the authorization protocols to realize the described capabilities. Section V provides concluding remarks and suggestions for further work.

II. BACKGROUND

A. 4G Systems Service Authorization Model

Since its inception in 3GPP Release 8, the Evolved Packet System (EPS) has adopted a service authorization model whereby any subscribed service available on a network is implicitly authorized for a registered UE. A default (bearer) service is provided automatically to the UE during a network attach procedure upon successful authentication.

Service authorization in Long Term Evolution (LTE) centers around a static Subscription Profile (SP). Essentially, the authorization matrix for each UE is stored in the Home Network (HN) and is downloaded to the Serving Network (SN) following UE authentication [2]. The SN then uses the received authorization matrix to authorize the authenticated UE for access to services provisioned in its SP. Standardization and adoption of this static SP based authorization model has been successful from an interoperability standpoint, when applied to a market with a limited set of services delivered over wireless networks controlled by one or two Mobile Network Operator (MNOs).

Incremental changes to decouple authentication from authorization have been introduced for some new services but only on a case-by-case basis within the constraints of existing LTE networks. For example, Proximity Services (ProSe) in 3GPP Release 12 and Cellular IoT (CIoT) optimizations in Release 13.

A systematic design approach where modular authorization functions and procedures may be used across multiple services is a key to future-proofing the emerging 5G system. Such an approach will allow 5G networks to cope with the expected, much broader diversity of network services delivered over multi-tenant NSs.

B. 5G Systems Service Authorization Work

1) 5G Standardization for NextGen Mobile Networks

Standardization efforts for 5G systems are currently ongoing [3][4]. In particular, the concept of an SP will continue to play a central role for service access authorization. However, a static SP based authorization approach may expose the following problems and limitations when applied to a 5G system context:

- The approach may not scale to adequately support the high diversity of expected 5G services or cater to the desire of MNOs to offer differentiated service offerings. This may lead to a situation where there is a higher risk of mismatch between services available in an SN and those described in the SP (from the HN).
- The approach may not be flexible enough to accommodate deployments based on a NS architecture, where multiple stakeholders and various trust models [5][6] may be involved in providing 5G network services. The role of multiple stakeholder infrastructure service providers poses a challenge for

5G systems to align the accounting and billing functions of the various stakeholders' systems with appropriate authorization functions for the services that are consumed by a user.

- Blanket and static pre-authorization of services may pose a risk to the network operator and stakeholders. A diversity of devices are expected to attach to 5G networks designed for specific vertical use cases. These devices require a limited set of service requirements and it's desirable to provide access to only the services required for the specific application context and prevent access to other services. For example, using a static SP may lead to over provisioning authorization for services, leading to potential denial of service attacks and malicious abuse of services. Conversely, under provisioning authorization may lead to loss of revenues for the MNO due to a poor user experience and under-utilization of the network services available.

2) Network Slicing: A New Dimension to Authorization

In a traditional LTE mobile network owned and operated by a single MNO, it was logical to combine the authentication and authorization functions at the Mobility Management Entity (MME). The use of statically provisioned authorization data in an SP was considered sufficient in order to achieve secure deployments with simple management and operation, rather than a dynamic or distributed alternative. Such a static authorization approach prevailed as the 3GPP architecture evolved to address optimizations related to operational cost and network performance for Radio Access Network (RAN) sharing [7] or Dedicated Core Networks [8].

In contrast to these earlier efforts, the emerging network slice paradigm - thanks to the flexibility of NFV [9] and SDN [10] building blocks - is anticipated to evolve the mobile network architecture into full support of multi-tenancy. This latter capability is crucial for future networks to accommodate new use cases catering to new players in various vertical industries, tighter alignment with business application services and Over The Top (OTT) providers' specific service requirements. It may also enable more cost efficient and dynamic service provisioning on behalf of network slice tenants that lease resources from infrastructure providers. As a result, the 5G mobile network may support a more distributed and dynamic authorization functionality to control access to a diversity of service offerings.

C. Related Work

There have been several efforts to develop standards for dynamic authorization for web services as well as for the IoT as part of the Internet Engineering Task Force (IETF) [11]. The OAuth framework [12] is one of the more widely deployed mechanisms for services offered over the Internet. An access token (e.g., JSON access token) is utilized, whereby, a service owner may provide an entity (subject) with access to a service (object) based on the claims made within the token.

III. Dynamic Service Authorization Architecture and Framework

A. Types of Services

We propose an authorization solution that evolves the current 3GPP SP based authorization mechanism to support not only existing implicit service authorization, which we refer to as Basic Services and as deployed in LTE but also escalating layers of dynamic service authorization, which we refer to as Restricted and Negotiated Services.

Dynamic authorization for services that go beyond a Basic Service set is addressed using concepts of Restricted and Negotiated Services. The service delivery mechanisms are captured in an enhanced SP offering an evolutionary path from the familiar LTE authorization approach centered around a simple inspection of the SP. The mechanism allows a subscriber to dynamically access 5G services that are not initially enabled as part of an SP (e.g., enable some optional services based on user session context, referred here as Restricted Services) or to align a service request with an SN offering/capability (e.g., provision a new service based on SN capabilities), which we refer to as Negotiated Services. By way of illustration of the authorization concepts we take as an example a roaming scenario or a multi-tenant scenario where a third-party infrastructure provider is offering services to a user.

1) Basic Services

A UE may request a service from an SN. Upon receipt of a service request by the SN, the UE's SP is inspected for the requested service. If the service is enabled and is a part of the Basic Services, then the subscriber is automatically granted access to the service. Basic Services are statically provisioned in current 4G systems.

2) Restricted Services

Restricted Services may be optional services in the UE's SP that may have some service flows enabled while other service flows may be disabled or turned off by default. These services may be considered as services that have a set of characteristics (Quality of Service (QoS), security etc.) that have been agreed upon between a HN and SN but where explicit supplementary authorization may be required to enable the services for a User. When an authenticated User requests access to a Restricted Service, a dynamic authorization is initiated and upon authorization, the Restricted Service is enabled in the SP. This explicit authorization enables fine-tuning of the SP and flexibility in enabling services on a per device basis and may be based on specific contextual information such as type of device, geographic area, subscriber plan information etc. Such a type of authorization is based on a Pull Model. Once the UE is authorized and as long the Restricted Service remains enabled in the SP in the SN, any subsequent request to access the service is granted automatically, similarly to the Basic Services authorization process (i.e. without any additional messaging towards the HN).

As an example, in the case of IoT systems, some basic connectivity services may be pre-provisioned in a UE as Basic Services and a wider set of services recorded as Restricted Services. An IoT service provider may be able to dynamically authorize a UE, for a specific IoT application, in the field after the UE is deployed. Such service-specific enabling protects the network from misuse of the IoT device subscription and restricts service usage to the agreed upon IoT services and policy settings. In considering the potential excess signalling due to dynamic authorization messages coming from an SN, an IoT service provider may implement a policy to provision Restricted Services that need to be authorized only once, for example, during the very first connection and for the lifetime of an IoT device.

3) Negotiated Services

A Negotiated Service is a service that may not be provisioned by the HN Operator in an SP and builds on the concept of Restricted Services. These services may be offered by an SN that caters to a specific set of service characteristics deliverable over a NS. When an authenticated UE requests a service, the SP is inspected and if it does not contain the requested service, either as a Basic or Restricted Service, then a dynamic negotiation may be performed to seek authorization for the requested service. For example, the requested service, as indicated within the UE's SP for Basic and Restricted Services, may not be aligned with services available over a basic NS of an SN. However, the requested services may be available as an optional additional service, over a second NS. An alignment of the services and appropriate authorization checks may be performed and negotiated between the SN and the SP whether it be the HN or a Data Network (DN) in a Local Break Out (LBO) setting. A dynamic service negotiation may be carried out to indicate the required service characteristics, such as 5G QoS Class Identifier (QCI), and receive a dynamic authorization.

In an alternative deployment scenario, service authorization based on a push model may be performed with an OTT service provider, DNN or HN to provide pre-authorization. Such an offering enables service scalability in terms of seamless inclusion of OTT service providers and multi-tenant service providers and to provide a broader geographic reach. In order to enable such an authorization to an SN who may then perform appropriate authorization decisions, the policies may be pre-negotiated and communicated by way of a Proof-of-Authorization (PoA) provisioned in the UE.

B. Use Case Example

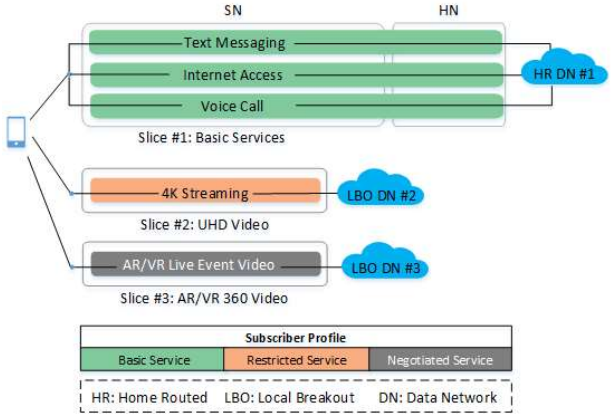

Figure 1: Example of Service Authorization over Network Slices

In order to illustrate the utility of the proposed authorization mechanisms for the various services, we consider the use case of a user going to a Sports Stadium to watch a game and upon arriving, wishing to access a video service while (s)he is waiting for the game to start. Illustrated in Figure 1 is an example of the user consuming various types of services over NSs provisioned by an SN. The Sports Stadium hosts a 5G network service and offers Basic services such as Internet access, texting and voice calls to the user, via the user's HN, without seeking authorization. The user request for access to the video service triggers a request to the user's HN for authorization to provide the video service. Once authorized, the services are delivered to the user. After the game has started, the user wishes to receive real-time live video from various cameras located around the stadium for a rich experience of the game. A request to deliver the service to the user is sought by the SN from the HN. Following the request and negotiation, upon receipt of the authorization, the user is seamlessly provisioned with the live video feed of the game. The dynamic request can be as simple as possession of an authorization token. Following activation of the App for the live video feed, an authorization from the user may be sought by way of a Terms and Conditions dialog box. Upon acceptance of the terms, a user consent authorization token is generated by the Sports Stadium. A recorded trace of the authorization information enables the Sports Stadium and the HN to settle accounts in a seamless manner, following consumption of the service by the user.

The Sports Stadium may host a RAN sharing infrastructure service with value-added services offered by way of a LBO service. The Sports Stadium has an arrangement with the SN to host and maintain the infrastructure. The first NS, provisioning such services as Internet access, texting and voice calls is classified as Basic Services, for which the authorization is provided via the UE's SP. A 4K streaming video service over a second NS is part of some Restricted Services recorded in the user's SP for which access is granted after the SN has sought authorization from the HN. Once authorized, the user's SP is updated with the authorization information and the services delivered to the user. A key feature of Restricted Services is that if the service is logged in the user's SP as "off" then the HN authorization is solicited whether in the context of a Home Routed (HR) or a LBO scenario, where data traffic is routed to/from a DN through the HN as a home routed service or through the SN by way of a LBO service. In contrast, Basic Services are automatically authorized based on a straightforward inspection of the SP provided by the HN during UE registration.

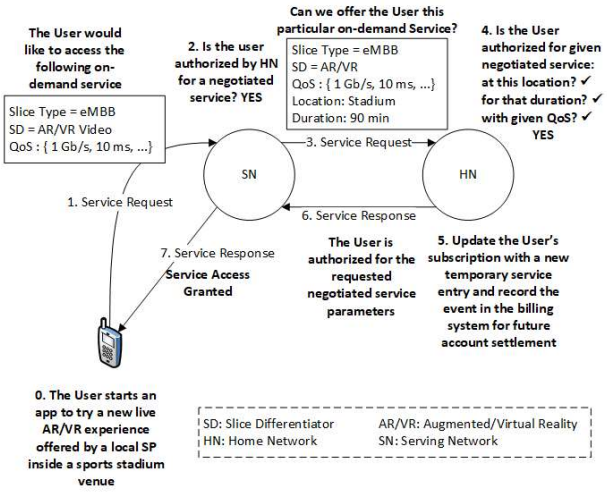

Figure 2: Dynamic Authorization for Negotiated Services

The Augmented/Virtual Reality (AR/VR) live video service is offered by the SN using a third dedicated NS, in an LBO configuration. As illustrated in Figure 2, upon request for the live video feed, the SN checks the user's SP and finds no authorization settings for this service. The SN then checks if the user has provided an authorization token and if the user is allowed to request negotiated services. The SN then initiates a request by sending an authorization request to the HN. The authorization function in the HN performs checks

on the user's profile, the authorization token, and the requested characteristics of the service to determine if the requested service can be delivered to the user. There may be a dialog between the SN and HN authorization functions to make adjustments to the duration of the offering and other information to arrive at a mutual agreement. Following a successful negotiation, the HN sends the authorization to the SN. Upon receipt of the authorization, the SN registers the authorization information for the user and provisions the user with the live video feed of the game. After concluding the service, the SN informs the HN of the service consumption information for later billing to the user.

C. Service Authorization Architecture

In the general descriptions that follow for an Authorization Function (AF), a UE wishes to access a service from an SN for which the UE does not have pre-authorization in its SP. The requested service is part of a Restricted Service or Negotiated Service that may require dynamic authorization for the specific service(s).

1) Service Access in the Home Network

In this scenario, a UE attached to its HN requests access to use a service provisioned by its HN. The request specifies a set of network services the UE is seeking from a specific slice type (e.g., eMBB, URLLC, MIoT) on behalf of a given application. Referring to an illustrative example provided in Figure 1 the network services "Internet Access" or "Messaging" may be delivered through the same eMBB slice but using service flows with different QoS characteristics (e.g. latency, throughput, delay) which the network is able to map to a particular QCI [3]. The HN AF obtains the subscription information from a Unified Data Management function (5G equivalent of Home Subscriber Server (HSS)) and local network authorization policies from a policy control function (PCF). As part of the authorization logic, the AF compares the set of service QCI from the UE request against the content of the SP matrix. The services description data may be conveyed by the UE by way of a Network Slice Selection Assistance Information (NSSAI) identifier or a Service Description Document (SDD) [13]. In the case of Restricted Services, some of these service flow parameters may be present in the SP but turned off by default and turned on through the authorization process.

In the case of Negotiated Services, some service flows may be absent from the SP and may be authorized on demand e.g., contingent on a supplementary authorization check, user payment confirmation. The AF may perform an SP check, apply operator policies, evaluate additional UE contextual information (such as location or time-of-day), and request additional information from the UE (e.g., user consent confirmation) in the decision-making process to authorize the UE for access to the service. Following a successful authorization, the appropriate network resource allocation and configurations are performed, and the UE may be granted access to the services over one or more NS.

2) Service Access in a Serving Network

A UE that is authenticated and registered with an SN, may request a particular service from the SN. The request specifies the service requirements similarly to the UE request in its HN, as described in the previous non-roaming scenario. The SN AF inspects the SP of the UE and forwards the request to the HN AF for service authorization since the requested service is part of a Restricted Service. Such a request allows the HN AF to administer network policies to authorize access to the optional service flows on a per UE basis. For example, referring to the example of Figure 1, the "4K Streaming" service may be authorized at home but require explicit dynamic authorization when roaming. In determining an authorization decision, the AF in the HN may also take into consideration contextual information (e.g. UE type, location, time of day). This Restricted Services model enables a very scalable, flexible, and agile architecture to dynamically authorize a particular service while a user is roaming or connected through a particular network in a LBO setting.

In the case of Negotiated Services (i.e., a service characteristic or feature not specified in the SP), the SN and HN AFs may enter into a negotiation protocol. For example, a service alignment may be performed between the services offered in the SN and those recorded in the SP by the HN and the service request mapped to a service in the SP and authorized by the HN. In an example, the service request may be offered by the SN in a separate NS, managed by a 3rd party infrastructure provider, that requires explicit authorization. The negotiation between the SN and the 3rd party may result in an authorization for the SN to provision the requested services to the UE. This procedure is to be contrasted with the previous scenario where the HN could unilaterally authorize the service request. Additional information from the UE may be obtained by the HN AF through the SN AF (e.g., user consent confirmation). Following a successful authorization, access to the service is provided to the UE.

IV. Detailed Solution

Figure 3 depicts a procedure for a Negotiated Service authorization procedure by an HN (i.e. A Home Public Land Mobile Network (HPLMN)) delivered through an SN (i.e. Visited PLMN (VPLMN)) in a 5G network environment.

The description of the steps is as follows (see Figure 3 for acronym definitions):

0. A UE has registered with the SN and as a result, the SN has obtained the UE SP from the HN and the UE has obtained information about the NS based services being offered by the SN.
1. The UE sends a request for an on-demand service provided by an SN but not provisioned by the HN in the User's SP. The corresponding single slice identifier (i.e. Single NSSAI (S-NSSAI)) may have been communicated by the SN via a prior message (e.g. Registration or Configuration). Referring to the example of Figure 2, the request may be triggered when the user starts a live AR/VR video app on his device while in the Sports Stadium. In the example, the given S-NSSAI comprises a standard slice type (eMBB) and a non-standard Slice Differentiator (AR/VR). The request is transported though the RAN to the AMF.
2. The AMF checks the User's SP to verify that the HN has enabled a capability to request Negotiated Services, since the request refers to a slice identifier (S-NSSAI) which is not provisioned by the HN in the User's SP.
3. The AMF forwards a Policy Check Request message to the Visited Policy Control Function (V-PCF) in order to determine the right set of policies (e.g. QoS, security policies) to provide the UE access to the requested NS.

4. The V-PCF determines that the requested NS does match the service / slices allowed for by the HN. The V-PCF sends a service negotiation request to the Home PCF (H-PCF) that includes a description of the negotiated Service Characteristics (e.g. QoS, Security policies). A standardized service definition template or fields format (e.g. standard QCI values) may be used for interoperability across various network domains.
5. Upon receiving the request, the H-PCF obtains the SP from the UDM
6. The H-PCF uses the HPLMN policy rules, the UE's subscription information, the requested service characteristics (e.g. QoS, security), the capabilities of the UE, any pre-authorizations, and the roaming agreements with the SN in order to determine authorization for access to the service.
7. Upon confirmation of the checks, The H-PCF records the authorization for the service including any contextual parameters such as a duration of the authorization in the UE's subscription information. In addition, such data may be recorded in the SN for faster re-authorization (e.g., for a subsequent request to use the service from the UE during the allowed authorization period).
8. The H-PCF sends a Service Negotiation Response message to the V-PCF that authorizes service delivery according to the selected service characteristics.
9. The V-PCF sends a positive Policy Check Response message that contains the authorization information including the accepted service characteristics to the AMF. The AMF selects the NS accordingly (e.g. the AR/VR Slice in Figure 1).
10. The AMF sends a PDU Session Request message to the appropriate SMF that is associated with the selected slice instance to perform service setup.
11. The SMF establishes a User Plane connection with the UPF.
12. The SMF also completes a User Plane setup in the RAN (via the AMF) and in the Core network.
13. The SMF replies to the UE via the AMF with a positive response.
14. The user proceeds to consume the AR/VR service provided by the SN.

V. Conclusion

We have presented a framework for providing dynamic authorization in 5G networks. The framework enables authorization and negotiation of a network service to requesting UEs/applications in 5G systems that include MNOs and 3rd party service providers. We introduced a concept of Restricted and Negotiated Services as an evolution of the current Basic Services that are based on the static Subscription Profile and authorization model of 3GPP. Restricted Services allow for fully standardized service definitions and persistence of existing pre-provisioning practices, in a similar fashion to existing Basic Services, but with the noteworthy advantage of accommodating dynamic service authorization. This capability is enabled due to the notion of optional service authorizations that may be turned on or off based on the context of the service request. These optional service authorizations allow the Home Network to gain more control of the authorization process when compared to existing LTE networks. Negotiated Services go even further, introducing a concept of dynamic service alignment between networks and opening the door for on-demand service enrollment and provisioning on behalf of the user. Further work to align the dynamic authorization architecture described here with 3GPP standardization efforts can benefit the adoption of rich application services in 5G systems.

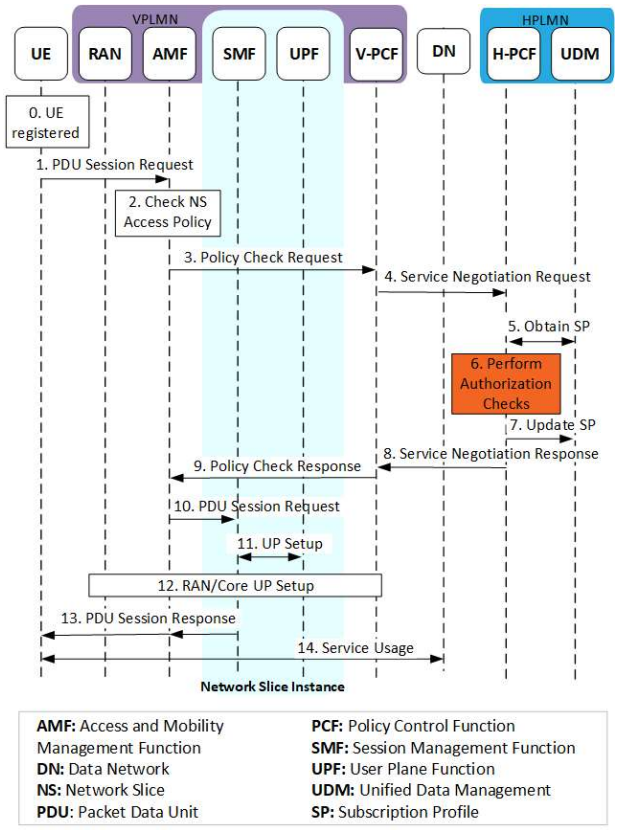

Figure 3: Negotiated Service Authorization 5G Mobile Network Call Flow

References

[1] Alliance, N. G. M. N. "5G white paper.": *Next Generation Mobile Networks*, White paper (2015).

[2] 3GPP TS 23.008, *Organization of subscriber data*

[3] 3GPP TS 23.501, *System Architecture for the 5G System*

[4] 3GPP TS 33.501, *Security architecture and procedures for 5G system*

[5] Huawei: *5G Security: Forward Thinking Huawei White Paper*: https://www.huawei.eu/sites/default/files/5G_Security_Whitepaper_en.pdf, 2015

[6] Ericsson: *5G Security Scenarios and Solutions*: https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-security.pdf, June 2017

[7] 3GPP TS 23.251, *Network sharing; Architecture and functional description*

[8] 3GPP TR 23.707, *Architecture Enhancements for Dedicated Core Networks*

[9] NFVISG ETSI: *Network functions virtualization, white paper,* 2012.

[10] O. N. Foundation: *Software-defined networking: The new norm for networks,* tech. rep., Open Network Foundation, 2012.

[11] IETF: *AAA Authorization Framework*, RFC 2904, August 2000

[12] IETF: *The OAuth 2.0 Authorization Framework*, RFC 6749, October 2012

[13] Vinod Choyi, Ayman Abdel-Hamid, Yogendra Shah, Samir Ferdi, Alec Brusilovsky: *Network slice selection, assignment and routing within 5G Networks*, IEEE Conference on Standards for Communications and Networking (CSCN), 2016