Proceedings of the of the 17th Conference on Computer Science and Intelligence Systems pp. 673–681
DOI: 10.15439/2022F55
ISSN 2300-5963 ACSIS, Vol. 30

Low-complexity access control scheme for MEC-based services

Mariusz Sepczuk, Zbigniew Kotulski, Wojciech Niewolski, and Tomasz W. Nowak
Institute of Telecommunications of WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland
Email: { m.sepczuk, z.kotulski, w.niewolski, t.nowak }@tele.pw.edu.pl

***Abstract*—The standardized security architecture proposed by ETSI for 5G networks provides six security domains covering network access and secure implementation of network services. However, this architecture does not specify detailed solutions for access control for web services and user credentials management. This paper proposes a new access control and service authorization protocol for the network services using MEC edge servers. Our solution does not slow down the performance of services in the 5G network. The advantage of this solution is that it allows you to solve some network security problems resulting from virtualization techniques (SDN and NFV) applied in constructing contemporary mobile networks.**

I. Introduction

THE FIFTH-GENERATION mobile networks are designed to provide network services with extremely high requirements in terms of bandwidth, the number of devices supported, latency, energy consumption, etc., see [1]. It enables the support of participants of mass events with good quality of service, the implementation of real-time services for telemedicine, monitoring and control of technological processes, and many others. However, it may not be possible to simultaneously meet all 5G quality requirements. Therefore, particular configurations of network services, called slices, have been proposed [2], [3]. In slices, the network parameters are adapted to the specific needs of a given application, for example, a virtual industry instance or its particular use case, see [4]. In order to effectively implement network slices designed for the needs of verticals in the 5G network infrastructure, it is necessary using virtualization techniques. 5G networks use SDN technology [5] to implement network traffic management and NFV technology [6] to enable flexible network deployment and dynamic operation. SDN and NFV technologies also allow the use of modern security solutions integrated with a centralized network controller, for example, the IDS / IPS system, see [7]. Another solution that allows improving network service quality is using edge servers with applications designed to support it. This solution is most effectively implemented with the use of MEC (Multi-access Edge Computing) technology, see [8].

Modern mobile networks of the 5th generation (and higher) are a result of the interaction of SDN and NFV virtualization technologies and MEC edge services technology [9]. From a functional point of view, we can call them 5G MEC networks; they combine mobile access to resources and services of high quality. Organizationally, such networks require the cooperation of many stakeholders participating in the implementation and use of web services. Ensuring the harmonious collaboration of all participants of the network services market while ensuring the necessary quality requirements and network limitations is a major technological challenge. However, providing the quality of a web service in 5G MEC networks cannot be at the expense of security. In particular, resource and service access protection methods can be a network service bottleneck. Therefore, an access control system adapted to the architecture of web services in 5G MEC networks is necessary for their proper functioning.

This paper aims to propose a new access control scheme for 5G MEC-hosted services that guarantees high service efficiency at a level of security similar to other modern network access control systems. It makes the network providers and the MEC-hosted service providers independent of external identity providers. It ensures strong user authorization to use services in the scope compliant with the applicable security policy. In addition, the system optimizes the operation of the network transmitting data related to the service. It also allows, if necessary, to interact with external identity providers in terms of primary user authentication. This system allows for the improvement of accessing services and granting permissions to users and increases the efficiency of the service implementation process.

The rest of the paper is organized as follows. Section II presents the standardized 5G security architecture and its basic access control domains. Section III reviews modern lightweight network authentication protocols that can be used for authentication and authorization on 5G MEC networks. Section IV presents the outline scheme of the 5G MEC access control architecture used in the special use-cases. Section V defines the optimized access control protocol for 5G MEC-hosted services. Section VI proposes possible improvements and optimizations of components, algorithms, and protocols supporting the access control system. Section VII presents the security advantages of the proposed solution and Section VIII concludes the paper and outlines the future work.

II. 5G networks and access control

The ETSI standard [10] proposes the 5G network security architecture. The architecture covers essential network security

This paper has been supported by The National Center for Research and Development, Poland, under Decision No. DWM/POLTAJ7/9/2020

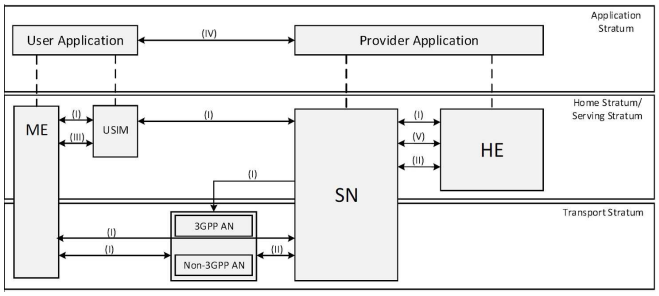

Fig. 1. Overview of the 5G security architecture [10].

elements, particularly network access control and network services access control.

Secure access to 5G MEC web services consists of two steps. The first one is secure 5G network access that enables a UE to authenticate and access the network securely (domain (I) in Fig. 1), including the 3GPP access and Non-3GPP access, and in particular, to protect against attacks on the (radio) interfaces, see [10]. This step is provided by network operators and is based on 5G standardized solutions. The second step is included in the application domain security (marked as domain (IV) in Fig. 1). It consists of security features enabling applications in the user and provider domains to exchange messages securely. This security area is in the competence of the service providers, particularly the MEC services providers. To ensure end-to-end security in 5G networks, the security architecture of the standard [10] should be significantly expanded. We must consider such elements as the end-user devices, the edge server services, and the computing cloud in which the service provider's resources are located in the network. Such an extended security model has been proposed in the paper [11].

The use of MEC technology in 5G networks facilitating the implementation of many services and improving their efficiency requires further expansion of the access control security model. In papers [12] and [13], we proposed a new security architecture with the integrated authorization mechanisms. Before we present our security architecture and the access control security protocols, we will briefly overview the contemporary access control solutions for the web services proposed in the literature.

III. Related work on the access control schemes

In mobile networks, the most popular method of access control and authorizing users in web services is applying external identity providers, such as Google, YouTube, Facebook, Okta, Microsoft Active Directory, etc. The offered solutions use well-known authentication and authorization protocols such as OpenId Connect, SAML (Security Assertion Markup Language), and OAuth 2.0. The OpenId Connect [14] is an open standard used for user authentication. It uses JWT (JSON Web Token) to deliver claims about the authentication of an end-user by an authorization server when using a client and other requested claims. SAML [15] plays a similar role but uses XML to exchange identity credentials and authorization data between identity providers and service providers to verify a user's identity and permissions. OAuth 2.0 provides secure delegated access. The application can take action or access resources from the server on behalf of the user without the user having to share its credentials. It does so by allowing the Identity Provider (IdP) to issue tokens to third-party applications with the user's consent. OAuth 2.0 [16] most often provides authorization services for users who have been authenticated using the OpenId Connect or SAML protocols.

An alternative solution to the authentication and authorization problem may be to use methods that do not require a central identity provider. These include verifiable credentials, decentralized identifiers, and blockchain. Verifiable Credentials (VC) [17] is an open standard for digital credentials. VCs contain such information as context, issuer, type, subject, and identity attributes or a cryptographic proof to ensure their integrity and authenticity. They can be expressed as JWT, see [18]. Decentralized Identifiers (DID) [19] is a type of identifier that enables a verifiable, decentralized digital identity. DIDs contain cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling independent controllers to prove to check the self-sovereign identity, see [20], [21]. Blockchain technology can be an alternative to decentralized authentication and authorization, see, e.g., [22].

In addition to authentication and authorization solutions for services in 5G networks, seen as mobile networks with general architecture, the literature offers proposals for solutions that consider the specific role of edge servers and MEC technology. It is proposed to provide access to enabler systems [23] or proxy servers [24] for user authentication and authorization. In order to improve data transmission, increase its security and improve efficiency, it is proposed to authorize the transmitted packets [25] additionally. Solutions of this type can operate independently or cooperate in identity delivery systems implemented by global suppliers, creating designs with high security, high flexibility, and the necessary autonomy in privacy.

In the literature, you can find works presenting access control protocols prepared especially for the 5G MEC network and services hosted in edge servers. For instance, paper [26] introduced a new access control protocol for the MEC system model and examined this protocol against user privacy requirements when sharing information that is not essential to the edge server-hosted service.

IV. 5G MEC access control architecture

Control of access to resources and services is an essential element of computer network security, and in mobile networks, it constitutes the basis for their protection. The access control system is the central element in our proposed 5G MEC network security architecture [12]. This section will outline this architecture, with its security domains and the core component specification. Our security architecture model consists of ten security domains that coexist and cooperate,

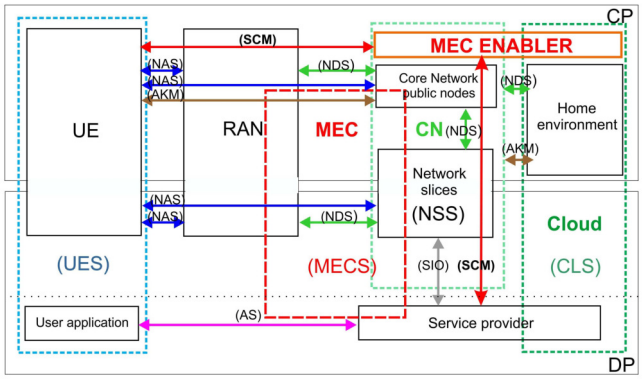

Fig. 2. The high-level access control security architecture in 5G MEC.

providing security services in all aspects of the 5G MEC mobile network functioning. It is related to basic the 5G security architecture presented in Fig. 1 and its extension proposed in [11], however, it contains components required by the MEC technology solutions. It is able to satisfy mobile networks security requirements enabling simultaneously to provide web services satisfying 5G networks' high quality expectations.

The 5G MEC security architecture designed in [12] consists of ten security domains. The number of the domains we consider is higher than those in [10], where six security domains for the 5G network are defined. This is because it must connect four network environments: 5G Core Network (CN), 5G Radio Access Network (RAN), the edge services provided by the MEC technology, and a new module which is the MEC Enabler, see Fig. 2. The domains of responsibility for security in the new architecture partially overlap with the areas proposed in [10]. To a large extent, they implement new security functions resulting from applications of the MEC technology and increase the number of stakeholders in the implementation of mobile network services. Below we present the security domains and their areas of responsibility, see Fig. 2.

- **NAS** (**Network Access Security**) provides basic security of user data. It includes confidentiality and integrity of signaling and user data between the User Equipment (UE) and the network in the Control Plane (CP) or the Data Plane (DP). It corresponds to the security domain (I) in Fig. 1.
- **NDS** (**Network Domain Security**) is the secure exchange of signaling and user data between different network entities. It corresponds to the security domain (II) in Fig. 1.
- **UES** (**User Equipment Security**): this domain contains software and hardware security at the user's side, including user access to the mobile equipment. It corresponds to the security domain (III) in Fig. 1.
- **AS** (**Applications Security**) is the support for secure communications between applications in UE and applications offered by the Service Provider. It is under the control of the end-user or the Service Provider (in the Application sub-Plane).
- **AKM** (**Initial Authentication and Key Management**): the security features that enable network functions to communicate securely. It includes mechanisms for authentication and key management that implement the unified authentication framework.
- **SCM** (**Security Credentials Management**) includes the service authentication and relevant key management between UE and the external data-transmitting network. In our model, the MEC Enabler governs this security domain.
- **SIO** (**Security Interoperability**) (also via MEC) is the support of the openness of security capability between the 5G network entity and the external Service Provider. It also includes the set of features that enable the stakeholders to know whether a security feature is in operation or not, which is defined as the security domain (VI) in [10].
- **NSS** (**Network Slices Security**) includes security of slices in terms like access control, authorization, and isolation.
- **MECS** (**MEC Security**): protection of Service Provider's software, virtualization platform (VM), and hardware supporting the edge server and the MEC host.
- **CLS** (**Cloud Security**) includes all solutions to secure resources and communication inside the cloud and the operator's home domain. This domain extends the resources offered by MEC-hosted services to the external cloud resources.

Two other security domains in Fig. 1 are the Application domain security (IV), providing the security features that enable applications in the user domain and the provider domain to exchange messages securely, and the SBA (Service Based Architecture) domain security (V), providing the security features that enable network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. In our model, their responsibility is distributed over AS, SCM, SIO, NSS, and MECS security domains because of the new important component, the MEC Enabler. The MEC Enabler acts as an AAA (Authentication, Authorization, and Accounting) server for all requests before any connection with MEC. Then, if the request is authorized, the MEC Enabler will properly control the configuration process of access to the MEC infrastructure and will create an information token that will enable to use of selected MEC services, see Fig. 3. The procedure of token creation and protection is an example of the solution analyzed and provided by ETSI (European Telecommunications Standards Institute) [10]. It involves the JSON (JavaScript Object Notation) Web Tokens with the appropriate digital signature, see the series of the RFC documents: [28], [29], [30], [31], [32]. This solution will reduce the management process and network resources' utilization for non-legitimate connections. The MEC Enabler will be responsible for service authentication and relevant

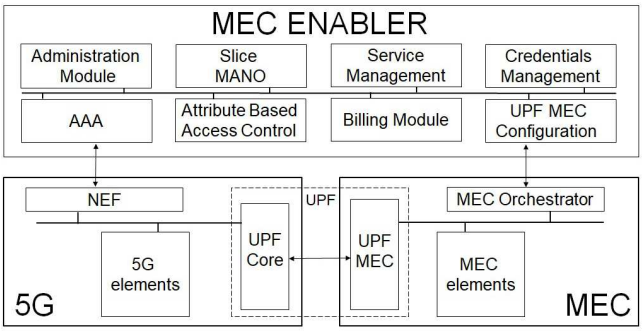

Fig. 3. The new network architecture with the MEC Enabler.

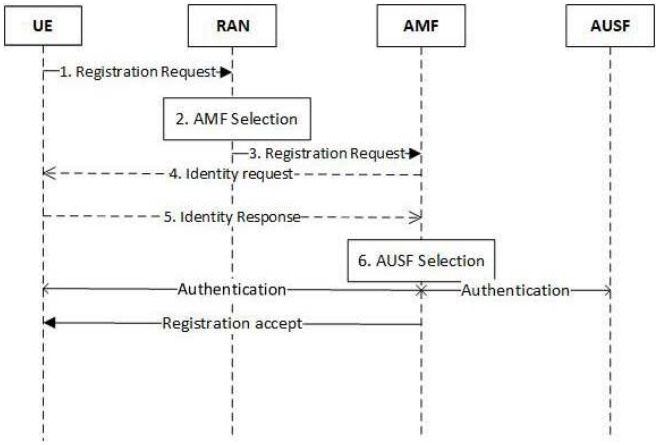

Fig. 4. Process of UE registration to the 5G network

key management between UE and the external data network realizing:

- services for legitimate users of the network,
- services for the secured communication (via slices or protected links),
- main security service for access to the MEC-hosted services,
- management of access rights by credentials,
- giving credentials to the progression of services considered as 5G MEC use cases,
- enabling services in the external operator's domain or over the cloud.

- **Administration Module**: this module supports all management operations and can configure other modules.
- **Slice MANO** (Management And Network Orchestration): the role of this module is to manage the slice life cycle in the MEC area. This manager can also reserve resources for specific slices and mark them according to service type, network identification, or any other rule, [34].
- **Attribute-Based Access Control**: this module stores all policy data about services, slices, available connections, and some other MEC information [35].
- **Service Management**: this module allows checking available services, their utilization, and the number of resources dedicated to them. The specific use cases can also manage the MEC's services lifecycle using MEC orchestrator API. However, it is also necessary to implement load balancing, which analyzes service placement [36].
- **Credentials Management**: this module creates tokens used for authorization of the MEC resources. This module's created token is monitored, refreshed, or deleted according to service needs [37].
- **Billing Module**: this module is dedicated to billing and storing information about MEC usage in different business models [38].
- **UPF MEC Configuration**: this module matches and adequately configures UPF MEC to link proper network slices with dedicated MEC resources [39]. When each slice represents another operator, this module establishes a connection between the operator and the MEC computation part assigned to it.
- **AAA**: this module is responsible for authentication, authorization, and accounting of all requests to MEC services [40]. After positive verification, UPF MEC Configuration Module prepares a network configuration that allows creating a connection with the chosen service, and Credentials Management generates a token for service authorization. Implementation of this module in the MEC Enabler will significantly improve the protection of Edge resources.

V. 5G MEC ACCESS CONTROL PROCEDURE

A. General access control to 5G network

The access control process includes three phases: UE registration to the 5G network, the discovery of proper UPF Core, and access to a MEC service. In the registration part, devices are verified whether they can be connected to the 5G network. In the discovery phase, the network must find a proper UPF that can communicate with the MEC network. Moreover, in this phase possibility of establishing a connection between UPF Core and UPF MEC is checked. Finally, access to selected MEC services is performed when the UPF Core can securely communicate with UPF MEC.

The diagram in Fig. 4 represents the communication flow in phase 1 when the UE tries to register to the 5G network. The flow in the registration phase was created based on the registration procedure shown in ETSI Technical Specification [49]. First of all, UE sends a registration request to the gNB (RAN) with all necessary information about UE (UE context), such as SUCI (Subscription Concealed Identifier), last visited TAI (Tracking Area Identity), Requested NSSA (Network Slice Selection Assistance Information) and many more. Then, the RAN chooses AMF (Access and Mobility Management Function). The AMF performs most of the MME's functions in the 4G network. One of these is UE authentication. AMF sends an identity request to the UE (optional request for additional data), and when it gets a response, AUSF (Authentication Server Function) performs the selection procedure. After that,

authentication messages are exchanged between the AUSF, AMF, and the UE. Finally, if everything goes correctly, the UE is registered as reported by the AMF.

In the phase of discovery proper UPF Core(see Fig. 5), authentication between UE and AUSF is first performed. After that, the AMF module sends a request to SMF (Session Management Function) to start the UPF Core discovery and a selection procedure. In the classical approach to the 5G MEC , network SMF is responsible for UPF management (e.g., configure traffic steering rules), so it must communicate with a new authentication and authorization service to ensure proper access control to MEC. To check if UE can access the MEC service, SMF, through NEF, sends a verification request to MEC Enabler (MEC EBR). The MEC EBR checks if UE via UPF CORE can establish a session with UPF MEC and if UE can use a particular MEC service. As a result of verification, a token is created. The token contains the necessary information as a result of two previous checks. If everything is going well and SMF receives the token, it sends the request to UPF CORE for an update session. Finally, after receiving a response about the correct data update from UPF CORE, a sequence of messages confirming the possibility of sending data from the UE to UPF CORE and UPF MEC is sent.

The final phase of access control to MEC service is internal access in MEC infrastructure (see Fig. 6). UPF MEC sends an application request to TMS (Traffic Management Service). The TMS is responsible for sending service access information to the MEC platforms. The MEC platform chooses adequate service and verifies the received token. After that, the MEC platform sends a request to the selected service; data from the service is sent to the UPF MEC and finally to the UE. In this phase, the proposed message flow is similar to the standard proposed in RFC 7519 for JWT tokens [32], making it easy to implement and use.

The descriptions above relate to the general assumptions made for controlling access to services in the 5G network. In the context of the 5G MEC network, the description should be detailed, and this will be done in the next subsection.

B. Steps of created access control protocol

Before accessing the resources hosted in the MEC environment, some steps should be taken (see Fig. 7). The proposed authorization process includes actions related to registration in the 5G network, which are the first condition for accessing the network [Step 1]. If the first access condition is met, the client will be correctly registered in the network, and then it will be able to try to connect to MEC resources. For this purpose, its request will be authenticated through the second step of the access control process, which verifies whether the request can be authorized by the access server dedicated to the application [Step 3]. After successfully passing the second step, the request is sent for the policy-based access verification [Step 5]. At this point, the access policy is checked based on the knowledge about the device's origin in the network and confirmation of the rights to use the indicated resource. Before making a decision, the policy-based access module considers many aspects, such as information about the slice from which the request is sent, a destination of the request, the user name, and more. Then, according to the stored policy, MEC Enabler decides whether to send the request to the application or not [Steps 6-7]. Suppose the request complies with the policy and in that case, the network element will be appropriately configured to enable connection from the device to the application located in the MEC [Step 8]. The exact course of the authorization process is presented in the points below:

1) The registration request is sent from the User Equipment (UE) RAN Access components:
   - The request is sent to the Access and Mobility Management Function (AMF)
   - Start of the Primary Authentication between UE and Authentication Server Function (AUSF) according to the 5G procedure
   - UE establishes NAS security context with AMF
   - UE initiates the establishment of a new PDU Session by sending NAS message
   - AMF selects V-SMF (Visited Session Management Function) and sends PDU Session context request
   - V-SMF sends PDU Session context response.
   - H-SMF (Home Session Management Function) obtains subscription information from UDM and verifies that UE's request is compliant
   - H-SMF sends EAP Request/Identity message to UE
   - UE sends EAP Response/Identity message
   - H-SMF selects UPF and establishes an N4 Session.
2) H-SMF forwards request to UPF
3) UPF forwards the request containing EAP Response/Identity message to the MEC Enabler AAA server (ME:AAA).
4) AAA module verifies if the sent data are correct. After positive verification, authorized data (user's contextual data and positive authorization) are sent to Slice MANO.
5) Slice MANO based on available resources information on local MANO slice resource database extends authorization data with the slice data such as priority of the request, identifiers of requested slice/slices, service localization
6) ABAC module checks data collected from Slice MANO in the context of one of the access policies located in a local ABAC policy database. Finally, slice data and ABAC verification information are forwarded to the Credentials Management module after positive verification authorization data.
7) Credentials Management entity creates JMAT token based on gathered data from ABAC entity. It sends it with configuration data (service localization, priority of handling requests, required types of UPF, slice ID, and network token) to the UPF Configuration module.
8) ME: UPF Configuration module based on configuration data from Credentials Management module sets network configurations on UPF Core and UPF MEC to establish

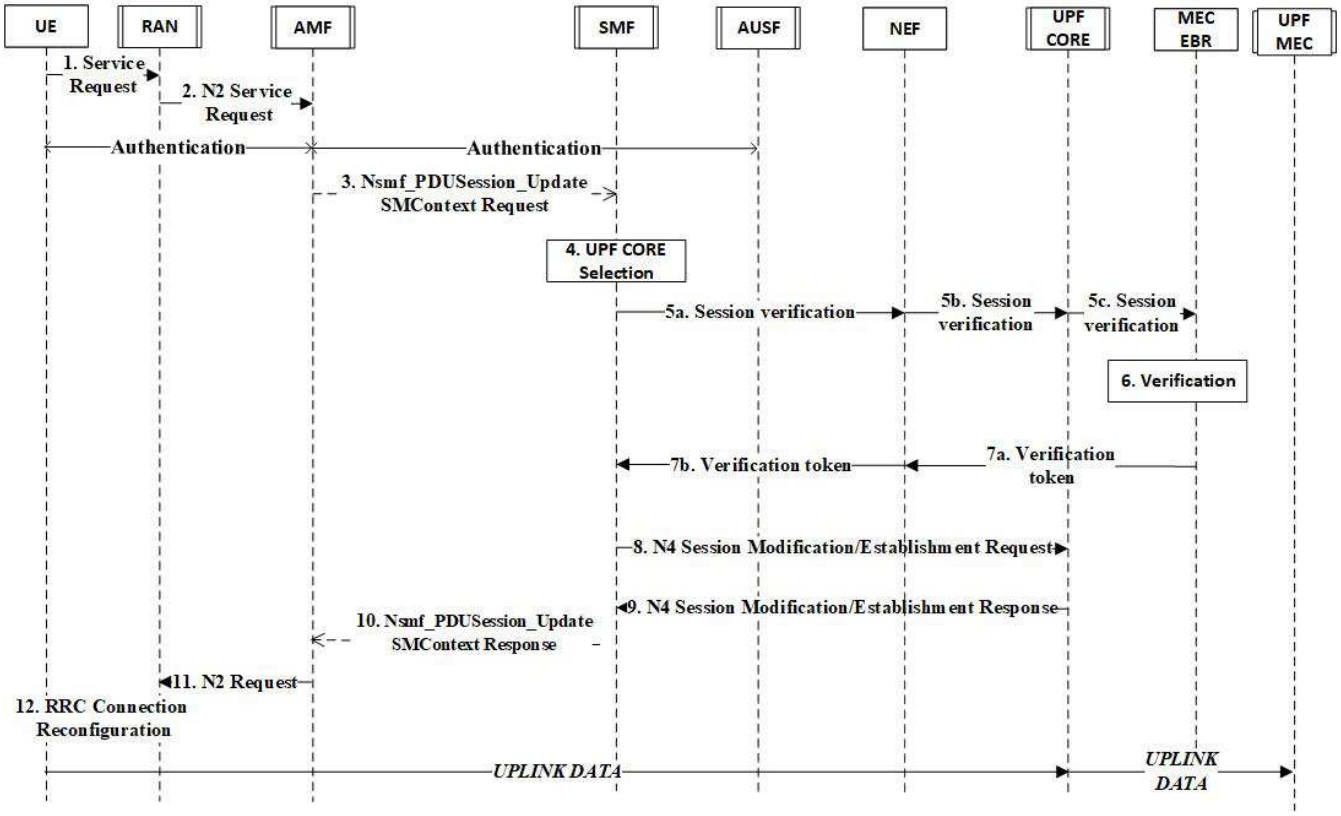

Fig. 5. Process of discovery proper UPF Core

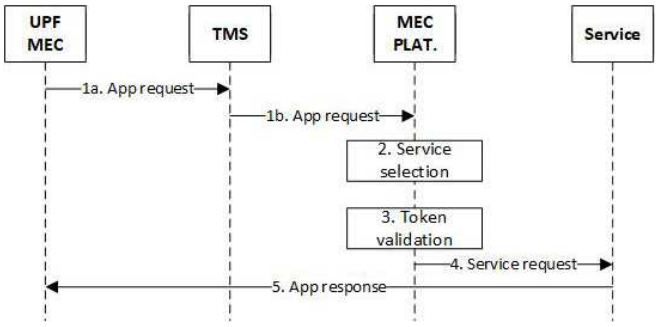

Fig. 6. General process of access to a MEC service

a connection to the service.

9) The request is transferred to the service located in the MEC environment.
10) UE establishes an End-to-End connection with the requested MEC:App.

As presented in the process description, the central role of the MEC Enabler in the authorization process is to add another access control step (based on verification of additional context information). This step increases the security of connection with the MEC environment and allows the protocol to be extended by other steps in the future. Currently, the policy verification process makes binary decisions - it may allow access or decline the connection.

Naturally, the data flow from Fig 7 shows the connection part to the MEC service, not the management of the established connection. In addition, the service access token must be verified for its validity (e.g., token lifetime, data validity in the token, etc.).

VI. Possible improvements and optimizations

This section describes entities that might be improved in the overall architecture presented in this paper.

A. JMAT token generation

In the past, during the design and implementation of JMAT tokens, we decided to improve its structure. The detailed results were described in [13]. Below are the key improvements that reduced the generation time:

- Reorganize the way of storing the data - we utilized a file system with directories and proper file naming as a data structure that exposes the quick find operation.
- Avoid JSON (JavaScript Object Notation) deserialization, also called JSON parsing - deserialization is a widely used operation in Object Oriented Programming, however it might be time-consuming. We decided to utilize the knowledge about the exact object structure that must be deserialized to read needed data.

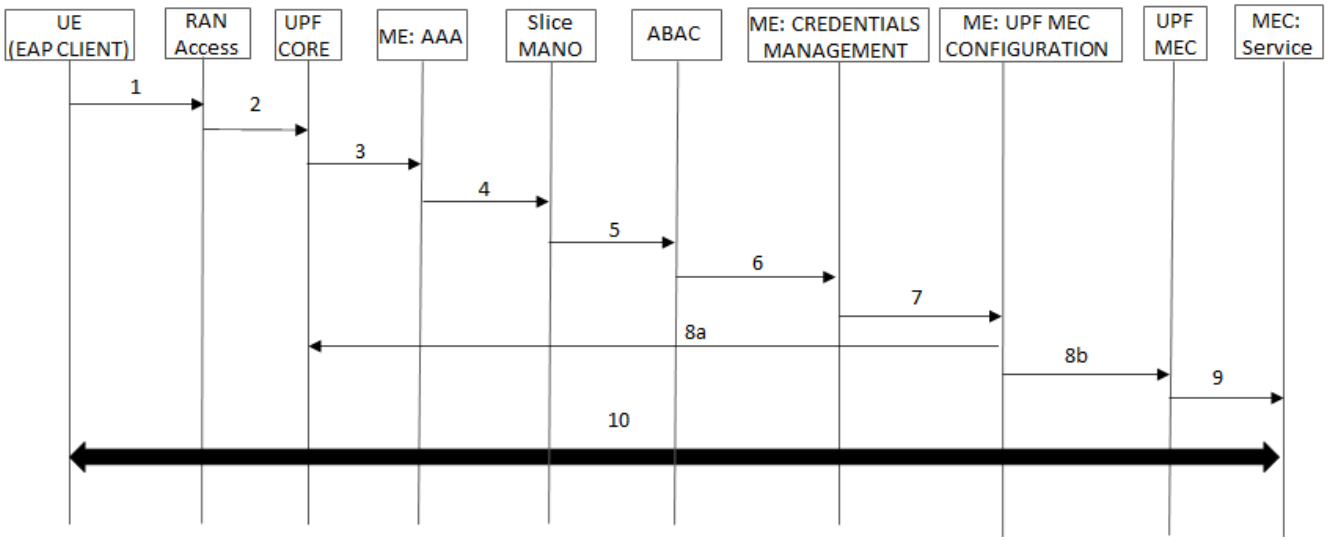

Fig. 7. Steps of created access control protocol

B. Py-ABAC rules and rule evaluation

We utilize ABAC (Attribute-Based Access Control) approach to manage access control to services for users. We use the py-ABAC library, described widely in [27]. Incoming requests might be denied or allowed with py-ABAC policies evaluation during Step 6 in the process in Fig. 5. The py-ABAC engine evaluates the final boolean decision (deny or allow the request) with rules stored in the memory or database. Each rule gives a boolean result, and the final result is calculated by n-ary OR or AND operation over those rules. In the worst scenario, the engine requires all rules to be evaluated to obtain the result. This algorithm could be improved by properly ordering the rules first to check those rules that determine the final decision. As a result, the average time needed for request analysis might decrease if rules are ordered properly. The first rule to evaluate might also be selected by a classification algorithm executed with the request's data and context.

C. Token verification after authorization

According to the concept of MEC Enabler, each first service request must be checked if it is authorized to the service and if it complies with the access policy. After passing the authorization process, an access token is generated. This token contains important information that confirms connection access to the service and data for authentication.

When the service implementation status does not change, the token validation causes unnecessary delays because the other parameters are the same apart from the token validity. Limiting the validation process only to check the token's validity would be sufficient.

When a service implementation status has changed, the token validation should be extended with additional policy verification. It would be sufficient first to limit verification with altered parameters and check if they fulfill policy needs.

The expected benefit is to reduce the time and resources needed for token validation. This approach might expose the authentication engine to some attacks based on token spoofing attempts or cheating the token policy.

D. Early evaluation

Incoming requests require authentication. The system could classify the request as pre-approved or pre-rejected based on the request's header and content (the early evaluation). When the request is pre-approved, the needed resources to establish the connection are collected, and the link is created before the request is authenticated and authorized. The expected benefit is the reduction of the latency for link creation. The main risk is the unavailability of needed resources for other valid requests due to pre-approvals. The classification algorithm might be applied here. Every decision made by the algorithm is validated by the authentication and authorization process, so with every request, the accuracy of the classification might be better. The over-learning problem should be addressed, e.g., by some data retention.

The approved request could be handled by MEC service or external (cloud) service. Thus, the early evaluation might return the following results: deny the request, take by MEC service, handle by cloud service.

VII. Security Aspects of the Proposed Solution

As we presented in the Introduction, the 5G mobile networks take full advantage of virtualization technologies (SDN and NFV) and the location of services in edge servers (MEC) to guarantee the highest quality of services. However, all these technologies require an innovative approach to the problem of network security and the security of MEC applications. On the one hand, virtualization technologies and shared infrastructure increase the network's vulnerability to attacks due to the openness of components that perform data transmission and other

network functionalities. Another issue is the fact that different stakeholders simultaneously use network functionalities. On the other hand, the transparent structure of the network with centralized traffic control allows the creation new level of security supervision. For example, a network controller with SDN technology can validate packages for different aspects. Consequently, it can be used to build a uniform decentralized IDS protection system covering all network nodes and supervising the correctness of packet flow, see [43]. In this case, responsibility for the entire system relies on the controller side. The problem of the effect of using programmable network technology on the network's security is extensively studied and has extensive literature, see, e.g., [44].

Among the various security methods proposed in the modern 5G MEC networks, an independent access control and user rights management system can significantly improve network security. The new access control architecture proposed by us, with the central element of the MEC Enabler, fully meets this expectation. It is compatible with network components belonging to different operators. Thus, in the control plane of SDN-based networks, a crucial vulnerability is the centralized single point control resulting in a global view of the network and exposing the underneath topology of a system [41]. In the literature, the proposed remedy is extending the Open Flow protocol to enable communication of the security policies between the security applications in the Controller to the agents in the switches, see [45]. In our solution, the MEC Enabler can improve the security of connections to the MEC by an additional layer of traffic control. Even when the MEC Enabler system is down, this will not impact the connectivity because the network without additional protection will be managed in a legacy manner (of course, in this case, security improvement done by MEC Enabler will not be available).

In the data plane, a critical vulnerability is that there is no standardized authentication mechanism in the switch for input traffic or incoming buffer data. Thus, erroneous flow alternation is possible. In the literature, the possible solutions could be using a covert channel defender (CCD), which can efficiently detect and prevent rule conflicts in the data plane, see [46]. It can also be an application of the access control scheme dedicated to a network distributed Intrusion Prevention Systems [47]. In our security architecture, the MEC Enabler can authenticate traffic based on JMAT tokens and, what is more, filter all traffic that has no valid token. Authentication done by MEC Enabler is multidimensional and includes more network information about connection such as slice, network provider, requested MEC application, and others.

Finally, a dangerous vulnerability is that there is no mechanism for identity control in the end-host/control channel. In the literature, the proposed solution can be cryptographic unique message identification for each LLDP packet, see [48]. The MEC Enabler can authenticate and check privileges for all MEC connections by analyzing the JMAT token. This type of access policy implemented in the MEC Enabler is essential for all edge systems. It protects its limited resources from unnecessary consumption and against dangerous attacks that automatically drop before reaching the MEC environment.

VIII. Conclusions and future work

In the paper, new access control and service authorization protocol for the network services using MEC edge servers was described. Firstly, we presented the standardized 5G security architecture and its essential access control domains. After that, the reviews of modern lightweight network authentication protocols that can be used for authentication and authorization on 5G MEC networks were specified. Next, we described the newly created access control procedure: starting with the characterization of MEC Enabler as the main element of the proposed solution, through the interaction of all 5G MEC network elements in the implementation of access, and finally presenting the advantages of the solution in terms of security.

In future works, we will focus on testing the created access control process for selected services in our experimental environment. We will extend the test bed with the implementation of new 5G MEC architecture components and prepare their verification in terms of the requirements enforced on 5G network services. Moreover, we plan to optimize the access control system according to several criteria, e.g., the applied resources and operations costs, its impact on QoS/QoE, expected risks and security level (Quality of Protection), etc. Finally, we would like to improve authentication mechanisms in the MEC Enabler by using Machine Learning algorithms for advanced policy analysis to reduce the time needed for the authentication and authorization procedure.

References

[1] *Minimum requirements related to technical performance for IMT-2020 radio interface(s).* Report ITU-R M.2410-0, ITU (2017)

[2] *Dynamic end-to-end network slicing for 5G*, Nokia White Paper (2016). Global mobile Suppliers Association. https://gsacom.com

[3] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2017, pp. 783-792, https://doi.org/10.15439/2017F228

[4] T.W. Nowak, M. Sepczuk, Z. Kotulski, W. Niewolski, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Verticals in 5G MEC-Use Cases and Security Challenges," IEEE Access, vol. 9, pp. 87251-87298, 2021, https://doi.org/10.1109/ACCESS.2021.3088374

[5] A.A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," Computer Networks, vol. 167, 11 February 2020, 106984. https://doi.org/10.1016/j.comnet.2019.106984

[6] ETSI GS NFV-IFA 010: *Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Functional requirements specification*,V3.6.1, ETSI (2022-01).

[7] F.N. Nife and Z. Kotulski, "Application-aware firewall mechanism for Software Defined Networks," J Network and System Management **2020**, vol. 28, pp. 605-626. https://doi.org/10.1007/s10922-020-09518-z

[8] Y. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, *Mobile Edge Computing. A key technology towards 5G.* **2015**, ETSI White Paper No. 11.

[9] B. Blanco et al., "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," Comput. Stand. Interfaces, **2017**, vol. 54(4), pp. 216-228, https://doi.org/10.1016/j.csi.2016.12.007

[10] *5G; Security architecture and procedures for 5G System.* ETSI TS 133 501 V16.5.0 (2021)

[11] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," SCIENCE CHINA, Information Sciences, **61** 081301:1-081301:25 (2018) https://doi.org/10.1007/s11432-017-9426-4

[12] Z. Kotulski, W. Niewolski, T. Nowak, M. Sepczuk, "New Security Architecture of Access Control in 5G MEC," in: *Thampi, S.M., Wang, G., Rawat, D.B., Ko, R., Fan, CI. (eds) Security in Computing and Communications. SSCC 2020.* Communications in Computer and Information Science, vol. 1364. Springer, Singapore 2021. https://doi.org/10.1007/978-981-16-0422-5_6

[13] W. Niewolski, T.W. Nowak, M. Sepczuk, Z. Kotulski, "Token-based authentication framework for 5G MEC mobile networks," Electronics, 2021, vol. 10, 1724. https://doi.org/10.3390/electronics10141724

[14] *Welcome to OpenID Connect,* https://openid.net/connect/

[15] *Profiles for the OASIS Security Assertion Markup Language (SAML)* V2.0 - Errata Composite, Working Draft 07, 8 September 2015, https://www.oasis-open.org/committees/download.php/56782/sstc-saml-profiles-errata-2.0-wd-07.pdf

[16] D. Hardt, Ed., *The OAuth 2.0 Authorization Framework,* RFC 6749, October 2012, Available online: https://datatracker.ietf.org/doc/html/rfc6749

[17] *Verifiable Credentials Data Model v1.1,* W3C Recommendation 03 March 2022 https://www.w3.org/TR/vc-data-model/

[18] N. Fotiou, V.A. Siris, and G.C. Polyzos, "Capability-based access control for multi-tenant systems using OAuth 2.0 and Verifiable Credentials," arXiv:2104.11515v2 [cs.CR] 28 Apr 2021 https://arxiv.org/abs/2104.11515

[19] *Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations,* W3C Proposed Recommendation 03 August 2021 https://www.w3.org/TR/did-core/

[20] A. Preukschat, D. Reed *Self-sovereign identity: decentralized digital identity and verifiable credentials,* Manning (June 8, 2021), ISBN-13: 978-1617296598.

[21] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital Identities and Verifiable Credentials", Bus Inf Syst Eng, vol. 63(5), pp. 603-613, 2021. https://doi.org/10.1007/s12599-021-00722-y

[22] N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, and G.C. Polyzos, "OAuth 2.0 authorization using blockchain-based tokens," arXiv:2001.10461v1 [cs.CR] 28 Jan 2020 https://arxiv.org/abs/2001.10461

[23] B. Liang, M.A. Gregory, S. Li, "Multi-access Edge Computing fundamentals, services, enablers and challenges: A complete survey," Journal of Network and Computer Applications vol. 199 (2022) 103308. https://doi.org/10.1016/j.jnca.2021.103308

[24] A. Ali, S.R. Khan, S. Sakib, S. Hossain, and Y.-D. Lin, "Federated 3GPP Mobile Edge Computing systems: a transparent proxy for third party authentication with application mobility support," IEEE Access, vol. 10, pp. 35106-35119, 2022. https://doi.org/0.1109/ACCESS.2022.3162851

[25] Sakthibalan Pandiyan, Devarajan Krishnamoorthy, "NRTAS: Non-redundant traffic authentication scheme for strengthening privacy in 5 G communication networks," Journal of Intelligent and Fuzzy Systems, April 2022. https://doi.org/10.3233/JIFS-212750

[26] G. Akman, P. Ginzboorg, and V. Niemi, "Privacy-Aware Access Protocols for MEC Applications in 5G," Network 2022, 2, pp. 203-224. https://doi.org/10.3390/network2020014

[27] *Project description: py-ABAC. Attribute Based Access Control (ABAC) for python.* https://pypi.org/project/py-abac/0.2.0/

[28] *JSON Web Signature (JWS).* RFC 7515 (2015) Available online: https://tools.ietf.org/html/rfc7515

[29] *JSON Web Encryption (JWE).* RFC 7516 (2015) Available online: https://tools.ietf.org/html/rfc7516

[30] *JSON Web Key (JWK).* RFC 7517 (2015) Available online: https://tools.ietf.org/html/rfc7517

[31] *JSON Web Algorithms (JWA).* RFC 7518 (2015) Available online: https://tools.ietf.org/html/rfc7518

[32] *JSON Web Token (JWT).* RFC 7519 (2015) Available online: https://tools.ietf.org/html/rfc7519

[33] *Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs*. 3GPP TS 23.222 V17.4.0 (2021-04)

[34] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Towards constructive approach to end-to-end slice isolation in 5G networks," EURASIP J. Information Security 2018, 2 (2018). https://doi.org/10.1186/s13635-018-0072-0

[35] W. Fisher, N. Brickman, P. Burdenet et al., *Attribute Based Access Control*. NIST SP 1800-3, Second draft (2017)

[36] B. Brik, P.A. Frangoudis, A. Ksentini, "Service-oriented MEC applications placement in a Federated Edge Cloud Architecture," in: *IEEE Int. Conf. on Communications (ICC), Dublin, Ireland, 2020*, pp. 1-6. https://doi.org/10.1109/ICC40277.2020.9148814

[37] P.A. Grassi, M.E. Garcia, J.L. Fenton, *Digital Identity Guidelines*. NIST SP 800-63-3 (2017). https://doi.org/10.6028/NIST.SP.800-63-3

[38] *Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements*. ETSI GS MEC 002 V2.1.1 (2018-10)

[39] *Multi-access Edge Computing (MEC). MEC 5G Integration*. ETSI GR MEC 031 V2.1.1 (2020-10)

[40] S. Behrad, E. Bertin, N. Crespi, "A survey on authentication and access control for mobile networks: from 4G to 5G," Ann. Telecommun. **2019**, vol. 74, pp. 593-603. https://doi.org/10.1007/s12243-019-00721-x

[41] R. Deb and S. Roy, "A comprehensive survey of vulnerability and information security in SDN," Computer Networks, Volume 206, 7 April 2022, 108802, https://doi.org/10.1016/j.comnet.2022.108802

[42] *NFV Security in 5G - Challenges and Best Practices,* ENISA Report, February 24, 2022, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices https://doi.org/10.2824/166009

[43] F. Nife, Z. Kotulski, and O. Reyad, "New SDN-oriented distributed network security system," Appl. Math. Inf. Sci. vol. 12, no. 4, pp. 673-683 (2018) https://doi.org/10.18576/amis/120401

[44] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A comprehensive survey on SDN security: threats, mitigations, and future directions," Journal of Reliable Intelligent Environments, 2022. https://doi.org/10.1007/s40860-022-00171-8

[45] K.K. Karmakar, V. Varadharajan, and U. Tupakula, "On the design and implementation of a security architecture for Software Defined Networks," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS),* 2016, pp. 671-678, https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0099

[46] Q. Li, Y. Chen, P.P.C. Lee, M. Xu, and K. Ren, "Security Policy Violations in SDN Data Plane," IEEE/ACM Transactions on Networking, vol. 26, no. 4, pp. 1715-1727, Aug. 2018, https://doi.org/10.1109/TNET.2018.2853593

[47] F. Nife, Z. Kotulski, "New SDN-Oriented Authentication and Access Control Mechanism," in: *Gaj, P., Sawicki, M., Suchacka, G., Kwiecien, A. (eds) Computer Networks. CN 2018. Communications in Computer and Information Science,* vol 860. Springer, Cham 2018. https://doi.org/10.1007/978-3-319-92459-5_7

[48] T. Alharbi, M. Portmann, and F. Pakzad, "The (in)security of topology discovery in OpenFlow-based software defined network," Int. J. Netw. Secur. Appl. 10 (2018) 01-16. https://doi.org/10.1109/LCN.2015.7366363

[49] ETSI Technical Specification, *5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 version 16.5.0 Release 16)* **2022**, https://www.etsi.org/deliver/etsi_ts/123500_123599/123502/16.05.00_60/ts_123502v160500p.pdf