The Case for Federated Identity Management in 5G Communications

Ed Kamya Kiyemba Edris
School of Science and Technology
Middlesex University
London, United Kingdom
EE351@live.mdx.ac.uk

Mahdi Aiash
School of Science of Technology
Middlesex University
London, United Kingdom
M.Aiash@mdx.ac.uk

Jonathan Kok-Keng Loo
School of Computer Engineering
University of West London
London, United Kingdom
Jonathan.Loo@uwl.ac.uk

***Abstract*—The heterogeneous nature of fifth generation mobile network (5G) makes the access and provision of network services very difficult and raises security concerns. With multi-users and multi-operators, Service-Oriented Authentication (SOA) and authorization mechanisms are required to provide quick access and interaction between network services. The users require seamless access to services regardless of the domain, type of connectivity or security mechanism used. Hence a need for Identity and Access Management (IAM) mechanism to complement the improved user experience promised in 5G. Federated Identity Management (FIdM) a feature of IAM, can provide a user with use Single Sign On (SSO) to access services from multiple Service Providers (SP). This addresses security requirements such as authentication, authorization and user's privacy from the end user perspectives, however 5G networks access lacks such solution. We propose a Network Service Federated Identity (NS-FId) model that address these security requirements and complements the 5G Service-Based Architecture (SBA). We present different scenarios and applications of the proposed model. We also discuss the benefits of identity management in 5G.**

***Index Terms*—5G; federated identity; service brokers; network services; security**

I. Introduction

5G will make network access more flexible, mobile subscribers with their User Equipment (UE) will be able to access the network services [1] via multiple wireless access technologies and UE authentication will be provided locally to access 5G services [2]. It will support multiple shareholders such as users, Mobile Network Operators (MNOs) and Service Providers (SP). 5G promises to provide seamless connectivity and secure access, which is a big challenge. Considering its multi-tiered nature, it is crucial for 5G to create a chain of trust between the UE, Home Networks (HN) and External Network (EN) like third-party SP (3P-SP) while implementing access controls. Such access controls must be able to identify and authorize the UE requesting access to 5G network services via different Access Networks (AN).

5G's enabling of multi-tenancy on the infrastructure through network slicing highlights the need for security contextualization propagation and sharing between MNOs and SPs. In addition, since 5G consists of multiple shareholders, it makes the implementation of access control at different levels and the interoperability difficult. While a Service-Oriented Authentication (SOA) and authorization mechanism can facilitate network slicing and service security providing quick access to network services and easy interaction between multiple shareholders.However, the security procedures and access policies may vary between networks, hence a need for a high level isolation between networks within the multi-tenant infrastructure and an integrated security mechanism. There is also a need to deliver services from multiple providers to users in a different security domains. Another challenge faced in 5G is unifying the Third Generation Partnership Project (3GPP) Authentication and Key Agreement (AKA) [1] framework with virtualization [3] framework for network access and network slicing provisioning. However, these two models could be unified by Identity and Access Management (IAM) through Federated Identity (FId) and Single Sign On (SSO) [4] implementation to complement the 5G objectives. 5G Infrastructure Public Private Partnership (5GPPP) suggested the use of federation of Identities (FId) over multi-tenant infrastructure [2] and while federated authentication mechanisms with a trusted 3P to protect network service access was suggested in [5] which could be used as part of Federated Identity Management (FIdM) in 5G. This would provide flexible security management, accurate tracking of relevant UE data and seamless connectivity. Where by HN and SP might delegate some of their security procedures and IAM to a 3P [6]. This also omits the need for secondary authentication protocol [1] every time the UE requests access to 3P Data Network (DN) services.

The architectural limitations, untrusted networks, multiple security domains and the need to provide users with variant of services, MNO might want to use 3P-SP to provide some services to optimize its own infrastructure [2]. In addition, IAM could be shared with other SPs for efficient security management and resources optimization. For instance, a 3P providing its own identity (ID), authentication and authorization mechanisms to UEs from another network accessing its network services.

Even though the related work discussed FIdM being a possibility in 5G for supporting UE accessing service in HN and EN. There is lack of a robust, unified, multi-purpose mechanism that addresses the security issues on authentication and authorization in heterogeneous network. There is also lack of mechanism that could provide a single digital ID

of a user for multiple SPs access from different security domains. With 5G Service-Based architecture (SBA), there is a need of SOA and authorization mechanism to secure network slicing. The challenge is how to guarantee the same level of protection for authentication and ID credential to the supporting technologies. FIdM has been discussed on network slicing provisioning [2], [5] and Internet of Things (IoT) [7], [8] but not on networks access and service authorization to the end user in HN or DN where we believe that FIdM will be an ideal solution to achieve seamless authentication and access control implementation.

Therefore, this paper first explores IAM and how the FIdM has been used to support identity management and how it could be used to support access to network services in 5G. It discusses how network service can be access via FIdM addressing authentication and authorization in 5G. It proposes a Network Service Federated Identity (NS-FId) model that complements the 5G system and security architectures. The proposed model facilitates authentication and authorization with SSO to access networks services from multiple SPs in a heterogeneous network. It leverages on 3GPP AKA mechanisms and Oauth2 framework to provide a FIdM for secure access to SP services. It also presents different scenarios that can benefit from the use of FId in 5G. And finally, it introduces different FIdM applications that can be adopted and used for different use cases supporting multiple networks, SPs and users in heterogeneous networks.

The rest of the paper is structured as follows, in section II related work on federated identity and security overview are presented. While section III presents IAM properties, FIdM and its related concepts. In Section IV, the proposed Ns-FId model in 5G is presented. We discuss benefits of FId in 5G in section V. We finally conclude in Section VI.

II. Related Work

Since 5G is still going through standardization, FId has not been integrated in 5G yet. IAM and FId in the provisioning of Network Function (NF) services were discussed briefly in [2]. While NFs and sharing of network services by MNO through a federated mechanism to allow each operator to offer specific NFs to the users as a service in a federation were presented in [9] but the access of service within the HN or from EN by UE using FId have not be explored yet. The focus on FIdM has been mainly on cloud services, social networks and IoT.

The authors in [7] explored IoT in 5G, they presented an identity federation mechanism that reuses the Subscribers Integrated Module (SIM) authentication for cellular IoT devices, enabling SSO features. While in [8], the authors proposed a federation model to support delay-sensitive applications for high-end IoT devices in 5G. An Identity Management (IdM) framework for e-health systems over 5G networks that provides mutual authentication and ID protection was presented in [10]. In [11], the authors proposed a method to secure communication that manages trust of IoT with a federated method while minimizing usage of resources in IoT devices in different domains each having separate trust authority. The authors in [12] discussed the use of FIdM and SSO to gain access to multiple services. An approach to achieve seamless mobility across heterogeneous networks based on FId system was presented.

The related worked in this section explored FId in IoT and heterogeneous networks in 5G via wireless access. However, most FId solutions focussed on the storing of data and security for accessing services on the cloud and social media. The FIdM for 5G is not well studied, even though FId for IoT on 5G has been investigated but does not cover security aspects of network services access, services authorization or network slicing in HN and 3P-SP which this paper intends to address.

III. Identity and Access Management (IAM)

MNOs are challenged with providing robust access controls, security and session continuity as users roam across different networks. In recent years, the IAM technologies have rapidly evolved to address security, user experience and privacy needs. The concept of SSO has been introduced in which a user may use a single set of authentication credentials to gain access to multiple services in multiple security domains. The SSO can be extended to enable authentication of users and their UEs for network access in 5G. The UE gets authenticated to the HN and SP, then gets authorized to access the services through security association and trust. With 5G promising to provide enhanced broadband, ultra-low latency and dense connectivity, UE authorization and handover through FIdM would allow smooth mobility across multiple networks. In addition, the UE won't have to go through multiple authentication procedures every time it requests to access services in multiple domains. There is a need for smooth transition from one domain to another while accessing restricted services, this can easily be achieved through IAM.

IAM system enforce access control to services and manage digital identities of users through FIdM. It identifies, authenticates and authorizes a user trying to access the network resources, services and applications. The user is given a single digital ID which is linked to multiple temporary or pseudorandom IDs associated to different user accounts. Each account can have different access controls and security context linked to a service. In addition, IAM manages access database, it can add, remove, update users' access rights and record user login information such as ID, keys and certificates. Some of the commonly used access management methods are SSO, Multi-Factor Authentication (MFA) and Privileged Access Management (PAM).

A. Federated Identity Management (FIdM)

In FIdM, multiple SPs can let subscribers use the same identification data to obtain access to different networks of resource owners in the multiple domains. The user accesses protected resources while the SP facilities the identification, authentication and authorization process handled by 3P such as Identity Provider (IdP). The IdP creates, maintains and manages identity information for users while providing authentication services to applications within distributed network. IdP

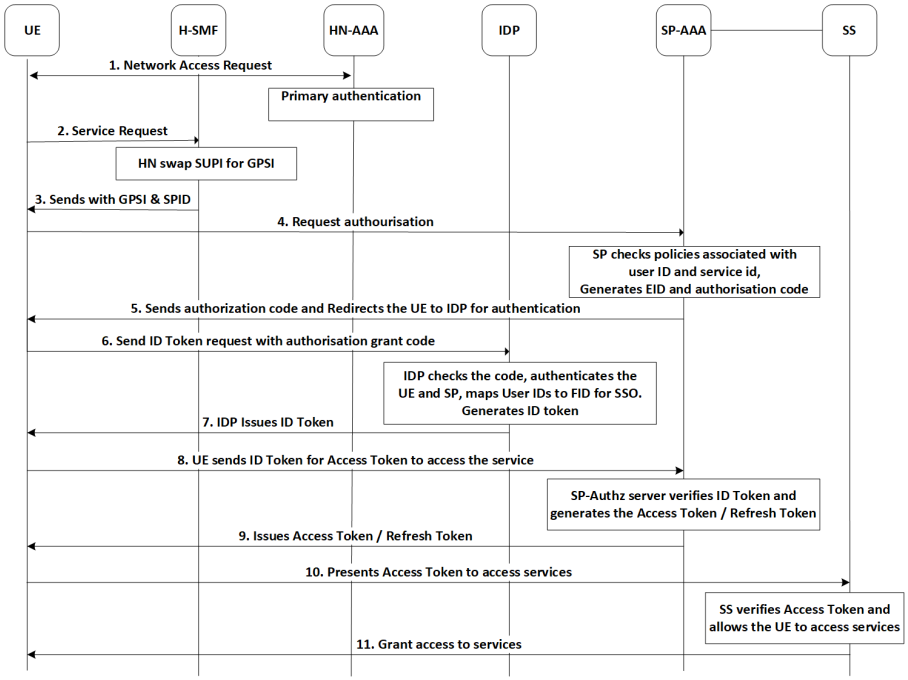

Fig. 1. 5G NS-FId Protocol Message Exchange Flow

also can facilitate connections between MNO/SP resources and the users, thus decreasing the need for users to re-authenticate when using mobile and roaming services. After successful authentication, the IdP transfers user ID and security context to the SP for access decision making [13]. Usually the IdP is based on a specific authentication method, the MNO and SP should also have various agreements and policies to facilitate the authentication and authorization of the users. Examples of SPs are MNO, Mobile Virtual Network (MVNO), Mobile Network Service Provider (MNSP) and Content Service Provider (CSP). The SP offers various services to users, they range from mobile network services, resources, content and OTT applications. FIdM makes the IdP's functions shared among several IdPs localized in different security domains. With IdPs and SPs in different domains, FIdM solves the single point of failure problem of the centralized IdM [10].

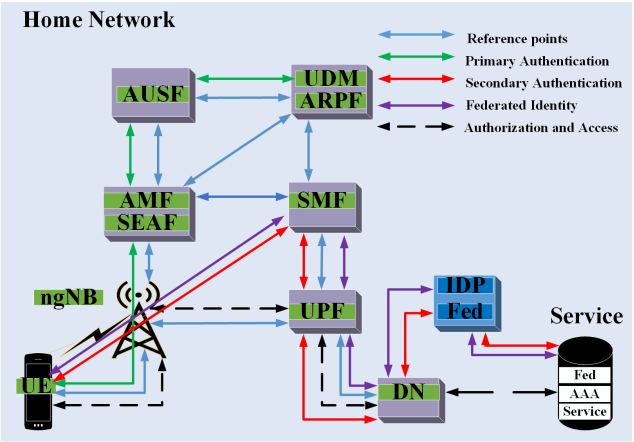

Fig. 2. Model A

With FIdM, the users get access to HN by authenticating through the home security domain. After authentication, the user initiates an attempt to get access to a service that uses identity federation then the service requests the user's authenticated credentials from authentication server. The authorization server authorizes the user to the remote services. Federation is used to manage and map users IDs between IdPs across organizations and security domains rely on PKI based trust and agreements in form of business, technical and policy pacts which must be in place. The SSO deals with authentication and the technical interoperability of the entities involved to provide the common login credentials across systems managed by IdP. Some of the FIdM entities include IdP authentication server, IdP identity database server, the SP authorization server, SP federation server and resource server. The FIdM relies on mechanisms such as SSO, SAML, Oauth2 and OpenID to carry out its objectives.

Single Sign On (SSO) allows a user to login and obtain access to multiple services of one network or more using a single set of authentication credentials. It is used for authentication and authorization processes that relate to the user's ID to provide access across multiple SPs. SSO allows a single authentication process to be used across multiple SP within a single network or across multiple networks. The system can generate and pass a trusted token around to different applications for authentication.

Security Assertion Markup Language (SAML) [14] is an open standard for authentication and authorization that de-

fines assertions protocols as assertion requests and responses between the SP and IdP, using standard communication procedure and profiles. It combines assertions, protocols and bindings that facilitates SSO. SAML defines a principal as end user trying to access a resource, the SP as server that the principal is trying to access. And an IdP is used to hold the principal's IDs credentials.

OAuth2 framework [15] is an open standard for authorization, provides secure delegated access, the client can access resources on a resource server on the behalf of a user without the user sharing their credentials with the resource server. It can also provide pseudo-authentication. In addition, it can be used to ensure that only authorized NFs are granted access to a service offered by another NF in 5G network [1] .

OpenID Connect [16] is another open standard for authentication, where a single ID is used for authentication of the user to a number of services. An OpenID Provider (OP) carries out user authentication like an IdP, using OpenID for authentication and OAuth2 for authorization. A user's ID is generally in the form of a URL, which is assigned by the OP and a Relying Party (RP) plays a similar role to as SP, providing access control functions to its resources.

B. Heterogeneous Network Service Access

Due to the heterogeneous nature of 5G, enhanced ID protection will be required as the UE accesses the network services via multiple access points. Mechanism such as pseudo-identifiers could be used to provide better anonymity against tracking of UE identifiers, but more advanced key management solutions are required to mitigate any effects of key leakage in 5G [2]. Traditionally MNO control the user's access and ID verification within the HN in a very controlled security context exchange process. However, 5G supports alternative UE IDs from semi trusted networks through Identity Management (IM) Domain which contains functionality to support alternatives to Universal Subscriber Identity Module (USIM) based authentication. While through 3P Domain and DN function, 3P can provide its own authentication and authorization to UE [2] in VN. That is why in 5G, a management domain was introduced to manage services security, security mechanisms, virtualized environments and UE domains. While IAM was introduced to address access control under Security Control Class (SCC), a collection of security functions to address access control, management of credentials and roles in 5G [2].

In order to identify and manage users' multiple IDs, the MNO could interact with the authentication entities of SP to authenticate the users via IdP, while it could also provide IAM services to 3Ps hence enabling ID interoperability among MNO and SP. UEs would be allowed to access services even in the cases where certain roaming agreements do not apply between different networks or device to device (D2D). Such use-cases could involve SP to provide services that could be accessed at the edge hence facilitating traffic offloading, improving latency, delay and relieve capacity overload on the network as promised by 5G. There should also be a stronger linkage between the user and their IDs to enforce accountability and non-repudiation in 5G. Similarly, non-repudiation assertion regarding compensation could be then given to the VN or SP [2].

In 5G, a Unified Data Management (UDM) function is used to manage users' data and profiles for both fixed and mobile access. The UDM function is required to be flexible and interoperable to unified device IAM hence can be supported by FIdM [17]. With IAM, the user proves its identity to the system for via multiple access points, using credentials such as user ID, cryptographic key, digital signature, digital certificate to the system then gets authenticated. Therefore, multiple digital IDs and FIdM can be key enablers for mobility, high availability of services and managing overlapping IDs from different domains that meets 5G specific requirements for the user, networks and SP. The services, ID verification, access control and attributes sharing are based on the trust between shareholders through federated delegation process. The level of security may vary depending on service and the security policies agreed between HN and the SP, to access services the UE may require a combination of cryptographic primitives and access controls for the authentication and authorization. FIdM solution could be used to provide secure authentication and authorization for network service access and delivery in 5G.

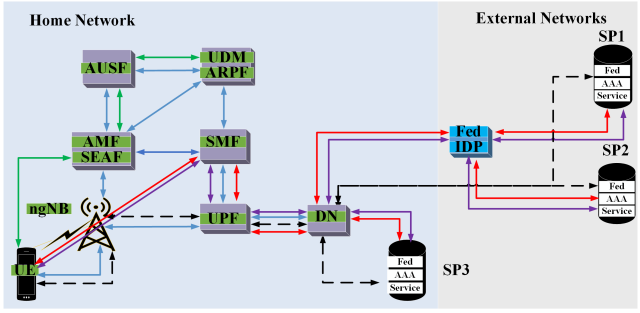

Fig. 3. Model B

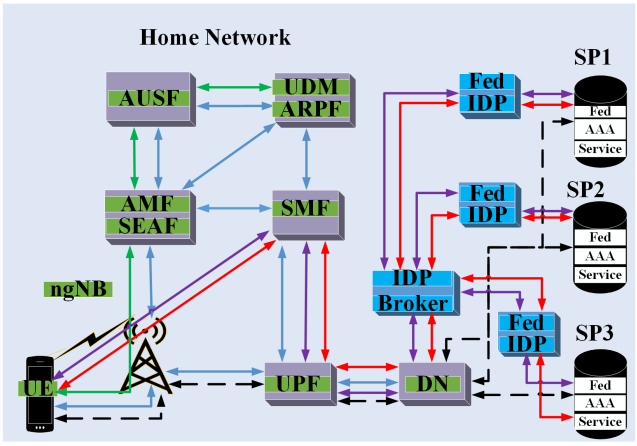

Fig. 4. Model C

IV. 5G Network Service Federated Identity (NS-FId) Model

5G requires an IAM solution, to support billions of heterogeneous UEs, network devices with variable security capabilities and attributes. Which would allow networks with an existing IAM solution to reuse it for 5G access. Moreover, new methods to handle UE's IDs with network slicing and enabling different IAM solutions per slice were defined in [2]. Therefore, FIdM can be applied along with SSO to support IAM in 5G. We propose Network Services Federated Identity model (NS-FId) that leverage on 3GPP system [18], security [1], SBA [19] and FIdM, to align it with the 5G standardization. The network services would rely on the user authentication process from a trusted IdP, using federated ID and SSO mechanisms.

A. Model Architecture

As mentioned earlier, with 5G standardization in late stages of development, there is still a lot of critical issues to be address such as authentication, authorization and IAM. Due to 5G's emphasis on not sharing the UE's Subscribers Permanent Identifier (SUPI) and other security context outside the HN, other methods must be considered to enable massive communication, seamless and secure connectivity when accessing services provisioned by the MNOs or 3P-SP. The proposed NS-FId model defines the following entities which might have more than one role:

- UE: The end user and principal accessing the service.
- H-SMF: The Home Session Management Function is 5G function that communicates with the HN-AAA and DN function or EN entities. Since the IdP and SP cannot interact directly with HN security entities
- HN-AAA: The HN Authentication, Authorization and Accounting (AAA) servers that carry out the primary authentication with UE and it consist of Authentication Server Function (AUSF), UDM and Authentication Credential Repository and Processing Function (ARPF).
- IdP: It provides FId, manages and carries out federated authentication and SSO. It verifies the UE, issue the FId and ID token. It hosts the active directory federated server and identity database.
- SP-AAA: It hosts the AAA servers owned by SP. The SP is also part of the transaction; It grants authority, issue access/fresh tokens to be used by the UE to access the service and exchanges Generic Public Subscription Identifier (GPSI) with External ID (EID). The EID is used in the secondary authentication or initial stages of federated authentication.
- Service Server (SS): The server that hosts the services, it grants access to the protected services.

We adopt federated AAA servers with 5G security architectures [1] entities to support FIdM. It allows the redefining of the UE ID parameters and sharing of security context in and outside the HN such as keys and IDs. The federated servers will store user's data that will assist the IdP in generating FId, federated authentication processes, which is complemented by the data stored in UDM hence supporting 5G security objective of minimal exposure of security context to ENs. The IdP federates UE IDs, carries out authentication of the user between MNOs to SPs, the FId is used as one security parameters in the generation of ID and access tokens for authentication and authorization to services respectively. The UE is required to follow the 5G standard for registration and authentication when accessing the HN and then FId authentication and authorization when accessing services from the HN and ENs. The model also introduces IdP Broker (IdPB) and SP Broker (SPB) to support FIdM:

- Identity Provider Broker (IdPB): It is an identity broker that connects the SPs with relevant IdPs in different domain, mapping identity attributes across multiple IdPs to a user, creating a trust relationship with between IdPs [20]. It acts as Security Token Service (STS) providers that can translate different tokens from one standard format to another. IdPB allows cross-platform federated authentication.
- Service Provider Broker (SPB): It has an affiliation with the SPs the user wants to access, it links the user with SPs in different security domains [21]. The SPB manages the communication with the user's HN to the SPs and links the IdP and SPs via IdPB. The SPB holds information about the services and connects the user to right SP hosting these services. The UE through HN requests access to the SP via the SPB which redirects the request to IdP or IdPB for authentication then to SP for authorization to access services. This model defines

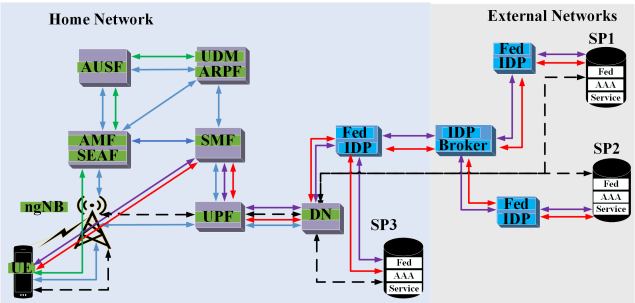

Fig. 5. Model D

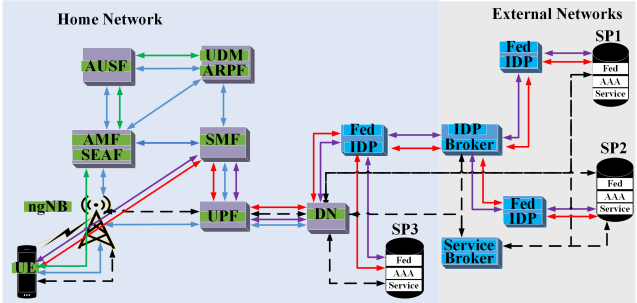

Fig. 6. Model E

three phases to complete a FId procedure; registration, authentication and Authorization.

B. Registration

The UE gets registered to the MNO prior to the initial authentication process, subscription data and security context are stored in UDM as per 5G standard. At the same time the UE's gets registered to SP databases with the necessary access polices and services agreements via HN. The MNO and 3P-SP must also register with the IdP, agree on the security parameters, PKI mechanism, polices, identities, authentication and authorization protocols to be used in the process. The SP registers the services, authorization policies, shared secret, SPID and credentials. While the HN registers the UE's GPSI, user attributes, HNID and credentials. Then the IdP shares its ID, creates users FId and shares it with MNO and SP.

C. Authentication

The first stage of authentication includes a primary authentication between the UE, Security Anchor Function (SEAF) and HN for the UE to access the network via wireless AN, initiated by SEAF and after successful mutual authentication the UE gets authorized to access the network [1]. 3GPP defined primary authentication procedure applied through Authentication and Key Agreement (AKA) mechanism with 5G-AKA or Extensible Authentication Protocol (EAP)-AKA' protocols as specified [1]. It involves the UE, Serving Network (SN) and HN but controlled by HN. In addition, a secondary authentication can also be used if requested by the SP for UE from other networks that are not registered to the same IdP as the SP to complete the registration phase. The secondary authentication is based on EAP framework, it involves the UE, HN and SP but controlled by SP [1]. The second stage of authentication uses the some of the security context, subscription data and GPSI from primary and secondary authentication procedures to complete a federated authentication between the UE, IdP and SP. The FId-based authentication is controlled by IdP where the UE is issued with FId and ID token to present to SP for authorization. The authentication methods and security context used depends on the registration data and agreement between the IdP, MNO and SP. After a successful primary or secondary authentication, IdP conducts a federated authentication, providing the UE with SSO to multiple SPs for authorization.

Furthermore, 3GPP developed the Generic Bootstrapping Architecture (GBA) protocol specification [22] to enable UEs to re-use the existing secure primary authentication procedures in order to gain access to the application services. The Network Application Function (NAF) with Bootstrapping Service Function (BSF) can be used to support this type of authentication. The BSF enables the NAF to verify whether a UE was correctly authenticated against the authentication vector located in UDM. This could also be used to support further federated identity assisted authentication procedures between the HN, IdP and SPs. The NF can securely expose security context, capabilities and events to 3P Application Functions (AFs) via Network Exposure Function (NEF) in 5G for authentication and authorization of AFs [1].

D. Authorization

With authorization, we adopt the Oauth2 framework [15] which is already standardized for NF application service access in 5G [1] and it an be integrated with an authentication procedure depending on the preferred authentication method and level of authentication required in FIdM. The UE credentials from authentication process are partly used for authorization grant codes with Oauth2. When the UE requests access, the SP issues the authorization grant and the Authorisation server issues access token to be presented to service server. An optional refresh token can be issued to the UE for use when the access token has expired, invalid or an addition access token is required [15]. The NEF can authorize requests from AF using OAuth-based authorization mechanism. However, with the use of FIdM, FId-based authentication method could be used after primary authentication [1] for an efficient interoperability process in heterogeneous network.

A generic and concise federated authentication and authorization message exchange flow of NS-FId model in Fig. 1 is explained below:

- Initiation: After a successful primary authentication, the UE requests to access to SP service through SMF, the SMF checks UE subscription and authentication data via UDM.
- Authorization Grant: After verifying the UE status with UDM, the SMF retrieves UE's GPSI and the SP's ID, send them to UE. It redirects the UE to the SP, which provides authorization grant code to UE and redirect the UE to IdP hence initiating federated authentication process.
- Identification: UE request ID Token from IdP by sending the authorization grant code, IdP assigns FId to the UE and maps it with other UE IDs and credentials.
- Authentication: The IdP checks if there is a need of secondary authentication or use the security context passed over by the HN/SP during registration stage. It verifies the UE then issues an ID Token. It maps the UE profile with MNO/SP attributes providing SSO.
- Authorization: The UE uses the ID token to request access/refresh token for access to the services. The authorization server verifies the ID Token and issues the access/fresh token to the UE.
- Access: The UE provides the access token to service server to gain access to the services, the access token is verified and the UE is granted access.

The UE will be able to re-use and renew the provided tokens depending on the polices, type of services requested and security parameters such as session expiration, suspicious requests and faulty process. The UE's SUPI should not be exposed to the ENs so IDs such as GPSI and EID are used where appropriate. The GPSI will be translated to the correspond SUPI in the UDM through SMF, EID through SP

and FID through IdP. Hence a universal recognition of the UE multiple digital IDs and enforcing federation practice in the HN and EN concurrently.

E. Use case Scenarios

FIdM in mobile network can take many forms depending on the network architecture and services provided. With 5G supporting multiple SPs such as MNO, MVNO, MNSP and 3P-SP, the relationship of the stake holders is based on trust using PKI mechanism. Different applications and scenarios in 5G are modelled as below:

- Model A: MNO and MNSP within a network trusting a single IdP as shown in Fig. 2.
- Model B: MNOs and SPs within a network trusting multiple IdPs through IdPB as shown in Fig. 3.
- Model C: MNOs and SPs across multiple networks trusting a single IdP as shown in Fig. 4.
- Model D: MNOs and SPs across multiple networks trusting an IdPB with multiple IdPs as shown in Fig 5.
- Model E: MNOs and SPs across multiple networks trusting an IdPB with multiple IdPs and SPB with multiple SPs across multiple networks as shown in Fig 6.

V. Discussion

The vast majority of the existing IAM solutions are based on assumptions that rarely apply to multiple domain with many providers and users. For instance, all involved entities must trust each other, data exchange is based on a specific protocol, and the end user is always capable of submitting the appropriate credentials to access restricted service in multiple domains. With network slices, multiple tenancy on the MNO infrastructure, tactile internet, IoT, edge services and restriction on sharing security context with 3P in 5G, IAM solutions that facilitates FId need to be considered.

In terms of network and service access, end user's authentication should provide SSO in heterogeneous networks like 5G. MNO should arrange FIdM with actors outside of their networks through IAM and trust relationships. The use of federation relationships between domains should be used for seamless authentication and authorization to variety of services. 5G should address security with unified multi-level security solutions using abstraction frameworks such as the one mentioned in press [23] as each level of the network and application have different security requirements and can be complimented by FIdM solutions. Through PKI trust with IdP, MNO/SP can choose an IdP, agree on policies, security parameters and mechanisms then direct the UE to IdP via IdPB for federated authentication services and before being authorized to access the services. Further data may be required to align the user's IDs, role and permissions related to access control provided in FIdM. In addition, the SPB is required to maintain connection of the SP target such IdP and other SPs. Our proposed NS-FId model defines mutual authentication, authorization, identity protection, secure access, interoperability and ease management of SSO. The integration of FIdM with mobile network can become part mobile network business model for implementing secure service authorization and prevent identity security breaches in networks.

VI. Conclusion

5G promises to provide seamless connectivity and support proximity services for mobile users via heterogeneous AN as well as enabling new network and service functions. It will create new use cases and connect vertical industries which require robust and interoperable IAM solutions. In this paper we explored the IAM and how the FIdM has been used to support identity management in cloud-based service, IoT and social platforms and how it could be used to support network services access in 5G. A federated model NS-FId that facilitates authentication and authorization with SSO to access networks services to multiple providers using FId in 5G is proposed. We also presented various FIdM models that can be adopted to support multiple networks, SPs and users in different scenarios. These models could be applied to fit different services provisioning scopes in any heterogeneous network. We finally discussed IAM and made a case for FIdM in 5G. The future work will focus on specification and formal analysis of security protocols that can be used in the proposed NS-FId model.

References

[1] 3GPP, "Security architecture; procedures for 5G system," 2018.

[2] 5GPPP, "Deliverable D2.7 security architecture (final)," 5G Enablers for Network, Tech. Rep., 2017.

[3] E. I. S. G. (ISG), "Network functions virtualisation (NFV); architectural framework," Unpublished, Tech. Rep. ETSI GS NFV 002 V1.2.1 (2014-12), 2014.

[4] G. Norma, "Ran architecture components – intermediate report," Tech. Rep., 2016.

[5] VirtuWind, "Deliverable D3.2 detailed intra-domain sdn & nfv architecture," Tech. Rep., 2017. [Online]. Available: /https://ec.europa.eu/research/participants/documents/downloadPublic/

[6] G. P. S. W. Group, "5G ppp white paper: Phase 1 security landscape," Tech. Rep., 2017. [Online]. Available: https://5g-ppp.eu/new-security-group-5g-ppp-white-paper-phase-1-security-landscape/

[7] B. Santos, B. Feng, and T. van Do, "Towards a standardized identity federation for Internet of Things in 5G networks," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2018, pp. 2082–2088.

[8] I. Farris, A. Orsino, L. Militano, A. Iera, and G. Araniti, "Federated IoT services leveraging 5G technologies at the edge," *Ad Hoc Networks*, vol. 68, pp. 58–69, 2018.

[9] J. Mwangama, N. Ventura, A. Willner, Y. Al-Hazmi, G. Carella, and T. Magedanz, "Towards mobile federated network operators," in *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2015, pp. 1–6.

[10] D. Fang and F. Ye, "Identity management framework for e-health systems over 5G networks," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[11] B. Anggorojati and R. Prasad, "Securing communication in inter domains internet of things using identity-based cryptography," in *2017 International Workshop on Big Data and Information Security (IWBIS)*. IEEE, 2017, pp. 137–142.

[12] Y. Targali, V. Choyi, and Y. Shah, "Seamless authentication and mobility across heterogeneous networks using federated identity systems," in *2013 IEEE International Conference on Communications Workshops (ICC)*. IEEE, 2013, pp. 1232–1237.

[13] E. Bertino and K. Takahashi, *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

[14] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott, and E. Maler, "Profiles for the oasis security assertion markup language (saml) v2. 0," *OASIS standard*, 2005.
[15] H. Dick, "The oauth 2.0 authorization framework," IETF, Tech. Rep., 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749
[16] O. Foundation, "Openid foundation — openid," 2007. [Online]. Available: https://openid.net/foundation/
[17] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.
[18] 3GPP, "System architecture for the 5G system," 3rd Generation Partnership Project, Tech. Rep., 2018.
[19] 3GPP, "5G system; technical realization of service based architecture," Tech. Rep., 2019.
[20] K. D. Austin, B. J. Schoppert, and M. Almond, "Identity broker configured to authenticate users to host services," 2013.
[21] G. Research, "Cloud services brokerage," 2013. [Online]. Available: http://www.gartner.com/it-glossary/cloud-services-brokerage-csb
[22] 3GPP, "Generic bootstrapping architecture (GBA)," Tech. Rep., 2018.
[23] E. K. K. Edris, M. Aiash, and J. Loo, "Investigating network services abstraction in 5G enabled device-to-device (D2D) communications," in *the 5th IEEE Smart World Congress*. Leicester, United Kingdom: IEEE, to be published.