Network Service Federated Identity (NS-FId) Protocol for Service Authorization in 5G Network

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—**Fifth generation mobile network (5G) will make network services available anywhere from multiple Service Providers (SP) and its provisioning raises security concerns. The users will require seamless connectivity and secure access to these services. Mobile Network Operator (MNO) will want to provide services to users and be able to share infrastructure resources with other MNOs. This requires robust authentication and authorization mechanisms that can provide secure access and provisioning of service to multiple users and providers in heterogeneous network. Therefore, Federated Identity (FId) with Single Sign On (SSO) could be used for seamless access and provisioning to network services in 5G. So, we propose Network Service Federated Identity (NS-FId) protocol, a federated protocol that provides secure access to services from multiple SPs and provides SSO to users. We formally verify and analyse the proposed NS-FId protocol using ProVerif. We also conduct a security analysis of the protocol's security properties.**

Index Terms—**5G; federated identity; security protocol; network services; authentication; authorization; access controls; formal methods;**

I. Introduction

In 5G, 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 (MNO) and Service Providers (SP). 5G promises to provide seamless connectivity and secure access, which is a big challenge. Considering its multi-tiered architecture, 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 (ACL). Such ACLs must be able to identify and authorize the UE requesting access to 5G network services.

5G's management of multi-tenancy on the infrastructure and network slicing highlights the need for security contextualization propagation and sharing between MNOs and SPs. Network functions (NF) and services can be shared between MNOs through a federated mechanism, to allow each operator to offer specific NF to the users in a federation [3]. 5G consists of multiple shareholders, which requires ACLs and interoperability at different levels of the network. There is a need of a robust authentication and authorization scheme to facilitate network slicing and service security for seamless access to network services and interaction between multiple shareholders. There is also a need to deliver services to users at the edge from different SPs and in different security domains. The challenge is unifying the Third Generation Partnership Project (3GPP) defined Authentication and Key Agreement (AKA) [1] framework with virtualization framework [4] and 5G Infrastructure Public Private Partnership's (5GPPP) suggestion of using federation of Identities over multi-tenant infrastructure [2] with authentication processes from a trusted 3P [5]. Federation of security would provide flexible security management, accurate tracking of relevant UE data and seamless connectivity. The MNO and SP would delegate some of its security management and Identity and Access Management (IAM) to 3Ps [6], in press [8].

MNOs are challenged with providing robust ACLs, security and session continuity as users roam across different networks. There is lack of a robust, unified, multi-purpose mechanism that addresses the authentication and authorization complexity in multiple domains scenario. There is also lack of mechanism that could provide a user with single identity (ID) to access service from multiple SPs from different security domains in 5G. Federated Identity Management (FIdM) has been discussed for network slicing provisioning [2] and Internet of Things (IoT) [7] but not for networks access and service provisioning, where we believe that use of Federated Identity (FId) and Single Sign On (SSO) will be an ideal solution to achieve robust authentication and ACL. Therefore, we propose a federated NS-FId protocol to provide a multi-level authentication and authorization to the UE for secure access and provision of network services across heterogeneous networks based on our initial work in [8]. It is complemented by 3GPP AKA mechanisms while leveraging on FdM and Oauth2 framework.

Our contributions are as follows; we explore how FId can be used to provide a universal ID in 5G and heterogeneous networks. We present a federated network access model that complements the 5G. We propose a NS-FId a federated protocol that can secure the access of services in HN and SP networks and achieve SSO for 5G. We model, formally analyse the proposed protocol using formal methods and automated proof verifier. We analyse the protocol and its security properties using two taxonomies.

The rest of the paper is structured as follows, in section II related work on FId, ACLs and formal methods are presented. While section III presents the proposed protocol, system model and security requirements of the proposed scheme. In Section IV, the modelling of the proposed NS-FId protocol is presented. We formal verify and analyses protocol in section V. In section VI, we analyse the security properties of the protocol. We finally conclude in Section VII.

II. Related Work

IAM and FId in 5G were discussed briefly in [2] and the focus on FIdM has been mainly on cloud services and IoT. The authors in [7] presented an identity federation mechanism that reuses the Subscribers Integrated Module (SIM) authentication for cellular IoT devices, enabling SSO in 5G. While in [9], presented a federation model to support delay-sensitive applications for high-end IoT devices in 5G within an integrated environment. In [10], an approach to achieve seamless mobility across heterogeneous networks based on FId system, pre-established application layer security association and access layer authentication are presented. In addition, the authors in [11] proposed a federated capability-based access control framework with delegation to enable an effective ACL processes to devices, services and information in IoT systems.

Some of related worked explored FId in IoT and heterogeneous networks. However, most FId solutions focussed on the data storage and access security on the cloud and social media. Even though FId for IoT on 5G has been investigated but does not cover federated security for network services access, services authorization and the proposed mechanisms are not formally analysed which this work intends to address.

A. Federated Identity

With FId, multiple SPs can let subscribers use the same identification to obtain access to services in their networks. The user accesses protected services while the SP facilities the identification, authentication and authorization process handled by 3P such as Identity Provider (IdP). The IdP creates, maintains and manages ID information for users while providing authentication services within distributed network. IdP also can facilitate connections between MNO/SP services 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's ID and security context to the SP for access decision making [12].

TABLE I
Core Language: Syntax and Informal Semantics

a, b, c, k, s	name
x, y, z	variable
M,N ::=	terms
h(D1, . . . ,Dn)	function application
f(M1, . . . ,Mn)	constructor application
D ::=	expressions
fail	failure
P,Q ::=	processes
out(N,M); P	output
in(N, x : T); P	input
!P	!P replication
0	nil
P — Q	parallel composition
new a : T; P	restriction
let x : T = D in P else Q	expression evaluation
if M then P else Q	conditional

Usually the IdP relies on a specific authentication method, the MNO and SP should also have various agreements and policies to facilitate the authentication and authorization of the user. Some of the mechanisms used in FIdM include Security Assertion Markup Language (SAML) [13], OpenID Connect [14] which provides authentication and authorization and OAuth2 framework [15] which provides authorization and SSO to user to access services on a service server. SSO enables a user to login and obtain access to multiple services using a single set of authentication credentials that relates to the user's ID in a single network or across multiple SPs. The SSO deals with authentication and the technical interoperability by providing common login credentials across systems managed by IdP. OAuth2 framework can be used in authorization of a NF accessing services offered by another NF in 5G [1].

B. Access Control

ACLs have been used to facilitate authorization in systems by granting a user access to an object, checked against the user's ID and a list of permissions [16]. Role-based Access Control (RBAC) [17] and Attribute-based Access Control (ABAC) [18] are some of the ACL mechanisms used to facilitate the granting of access rights and attributes to a subject for accessing an object. Other mechanism such as Encryption-based Access Control (EBAC) [19] have been implemented to provide an additional layer of security using cryptography. However, these conventional mechanisms alone are not enough to provide security for authorization in 5G due to its characteristics of massive connectivity, multi-tier infrastructure and heterogeneity. Moreover, it is inappropriate to implement security policies that require interpreting complex and ambiguous applications as it will end up increasing the effort and complexity on policy management as the number of devices grow in a multiple domains environment. In addition, Capability-based Access Control (CBAC) [20] approach has been considered as another solution, where a subject possesses a capability that references the object, using a capability token to grant the subject the capability to access the object [16].

C. Formal Methods

Formal methods and automated verification have been applied to authentication protocols for mobile networks to assess security properties [21], [22], to provide strong security guarantees. Security protocols properties are very challenging for most verification techniques and tools. This is due to the use of cryptographic primitive; its algebraic properties are tricky for symbolic reasoning [23] hence the certain tools, manual proof checks are not suitable. There are many automated verification tools that can be used for protocol analysis such as Automated Validation of Internet Security Protocols and Applications (AVISPA) [24] and ProVerif [25].

ProVerif analyses the security of cryptographic protocols, with Dolev-Yao models [26], it supports equational theories defined by a user and permits the verification of a variety of security properties. It uses applied π calculus [27] as a formal language for describing and modelling protocols. In addition, ProVerif supports cryptographic primitives defined by rewrite rules and equations that satisfy the finite variant property. The syntax is coupled with a formal semantics to allow reasoning about protocols, syntax and grammar in Table I. It also takes the security properties such as authentication, secrecy and observational equivalence to be proved as input. Cryptographic primitives are modelled as functions, messages as terms, built over an infinite set of names, variables and function symbols. For those reasons we find ProVerif a suitable tool for our analysis. It has been used to formally check security properties guarantees of authentication [28] and federated [29] protocols.

III. Network Services Federated Identity (NS-FId) Protocol

We propose a Network Services Federated Identity protocol (NS-FId) that leverages on 5G system [30], security [1] and SBA [31] with FIdM and ACLs supporting network services and network slicing provisioning as defined in [2]. To access the network services, the UE would rely on NS-FId protocol for authentication process controlled by a trusted IdP, using after this process they would be assigned federated ID and provided with SSO. The users get access to HN by authenticating through the HN security domain.

A. System Model

The proposed NS-FId protocol is based on FIdM model [8] as shown in Fig. 1 that incorporates 5G entities [1] with federated entities and can be implemented within the 5G core network (5GC) or in the 3P network. We adopt federated IdP servers, 3P-SP Authentication, Authorization and Accounting (AAA) servers and service server with 5G entities to support FIdM. It allows the redefining of the UE identity parameters and sharing of security context in and outside the 5GC such as keys, token, nonces and IDs. We define the following entities which might have more than one role:

- UE: It is the end user and principal accessing the service.
- H-SMF: The HN Session Management Function (SMF) is a 5G function that communicates with the HN-AAA and EN entities such SP authenticator, it acts as pass through authenticator.
- IdP: It provides, manages FID and carries out federated authentication and SSO. It verifies the UE, issues FID and ID token. It hosts the federated server and IDs 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).
- Service Server (SS). The server that host the services, it grants access to the protected services.

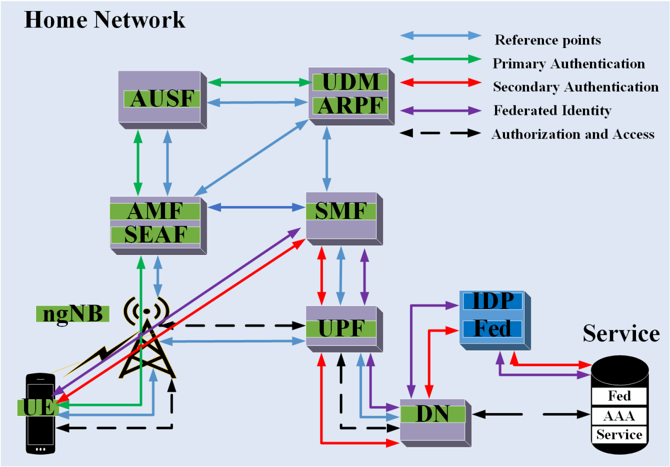


Fig. 1. 5G NS-FId Model

The Unified Data Management (UDM) function in 5G will manage users' data and profiles, it should be flexible and interoperable to FIdM [32]. The federated servers store user's data that will assist the IdP in implementing FId processes, complemented by the data stored in UDM. The user proves its identity to the system via multiple access points, using credentials such as user ID, cryptographic key, digital signature, certificate then gets authenticated. The services, ID verification, ACL and attributes sharing are based on the trust and security association between shareholders through federated delegation process. The UE follows the 5G standard for registration and authentication to access the network and then FId authentication and authorization to access services from the HN to Data Network (DN)/EN.

The UE gets registered to the MNO prior to the initial authentication process, subscription data and security context are stored in UDM. Contemporaneously the UE's gets registered to SP databases with the necessary access polices and services agreements by HN. The MNO and 3P-SP must also register with the IdP, agree on the security process, Public Key Infrastructure (PKI) mechanism, polices, identities, authentication and authorization protocols to be used. The SP registers its 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 and creates users FID and shares it with MNO and SP.

B. Security Requirements

Our threat model assumes a Dolev Yao (DY) adversary model [26], it controls the network, can read, intercept, modify and send messages. It is also capable of initiating passive and active attacks such as eavesdropping, manipulation, interception, impersonation and injection of messages. The adversary can also apply hashing, encryption and sign on values that are known to the attacker. The security properties are informally defined before the formalization of the protocol properties, we adopt the taxonomies in [33] and in [34] for precise formal analysis, referred to as set 1 and set 2 respectively in this paper:

- Set 1: The security properties in this set are specified from an agent A's point of view, with four levels defined between two agents A and B; aliveness, weak agreement, non-injective agreement and injective agreement.
- Set 2: The AKA protocol should meet the following security properties; mutual entity authentication, mutual key Authentication, mutual key confirmation, key freshness, unknown-key Share and key compromise impersonation resilience.

C. Authentication and Authorization

The first stage of authentication includes a primary authentication between the UE, Serving Network (SN) and HN for the UE to access the network provided by 3GPP 5G-AKA or Extensible Authentication Protocol (EAP)-AKA protocol' under the control of HN [1]. In addition, a secondary authentication can also be used if requested by the SP for UE from 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 some of the security context, subscription data and GPSI from primary authentication to complete a federated authentication between the UE, IdP and SP controlled by IdP. At the end of the authentication the UE is issued with an ID token and SSO. The SSO concept can be extended to enable single authentication for users and their UE to access services in 5G and other security domains.

With authorization, we adopt the Oauth2 framework [15] which is already standardized for NF application service access in 5G [1]. The UE credentials and security context from authentication process are partly used for authorization grant codes with Oauth2. The access permissions and attributes are extracted from the authorization policies under the user's profile to generate authorization grant and access token. When the UE requests access to services, the SP issues the authorization grant for authentication process and the authorization server issues access token for service access authorization. An optional refresh token can be issued to UE when the access token has expired, invalid or an additional access token is required [15]. We adopt some features from ABAC, CBAC and EBAC whereby the UE and the service objects are assigned a set of permissions in form of attributes and capabilities with encryption features integrated in a security token called NS-FIdACap. These permissions are created and managed by the SP and delegated to other entities such as SPAAA, IdP and SS. The SP sets up attributes and capabilities in relations with agreed policies with the UE's HN. It also assigns and manage permissions to UE (subject) and the services (Objects) together with the trusted authorities in form of security tokens. The security token's access rights, parameters, claims and format of ID and Access Tokens may vary but the main structure is the same, some are listed below:

- Token ID: It identifies a security token.
- Issuer: The entity that issues the token, signed with its private key.
- Issue time: Timestamp when the token was issued.
- Issue sign: This field for the digital signature of the token.
- Subject: The UE identity to which the rights from the token are granted.
- Service: The address of SP to which the token applies.
- Audience: The entity that token is intended for.
- Nonce: random nonce for authentication
- Expiry time: The time when token expires.
- Access right: Set of attributes and capabilities.
- Scope: Set of conditions that must be fulfilled like grant type, offline access, token type.

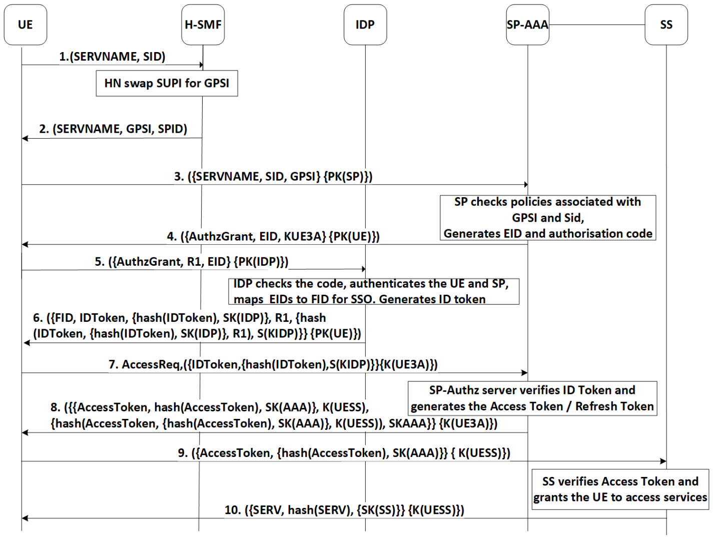

UE
H-SMF
IDP
SP-AAA
SS
1.(SERVNAME, SID)
HN swap SUPI for GPSI
2. (SERVNAME, GPSI, SPID)
3. ({SERVNAME, SID, GPSI} {PK(SP)})
SP checks policies associated with GPSI and Sid, Generates EID and authorisation code
4. ({AuthzGrant, EID, KUE3A} {PK(UE)})
5. ({AuthzGrant, R1, EID} {PK(IDP)})
IDP checks the code, authenticates the UE and SP, maps EIDs to FID for SSO. Generates ID token
6. ({FID, IDToken, {hash(IDToken), SK(IDP)}, R1, {hash (IDToken, {hash(IDToken), SK(IDP)}, R1), S(KIDP)}} {PK(UE)})
7. AccessReq,({IDToken,{hash(IDToken),S(KIDP)}}{K(UE3A)})
SP-Authz server verifies ID Token and generates the Access Token / Refresh Token
8. ({{AccessToken, hash(AccessToken), SK(AAA)}, K(UESS), {hash(AccessToken, {hash(AccessToken), SK(AAA)}, K(UESS)), SKAAA}} {K(UE3A)})
9. ({AccessToken, {hash(AccessToken), SK(AAA)}} { K(UESS)})
SS verifies Access Token and grants the UE to access services
10. ({SERV, hash(SERV), {SK(SS)}} {K(UESS)})

Fig. 2. 5G NS-FId Protocol Message Exchange Flow

TABLE II
NOTATIONS AND DESCRIPTION

Notation / Messages	Description
IDPID	IdP Identifier
SPID	SP Identifier
SID	Service Identifier
K(X)	session key
R1	Random Nonce challenge
EID	UE External Idenitfier
FID	UE Federated Identifier
GPSI	UE Generic Identifier
IDt	ID Token
PK(x)	Publci key
SK(x)	Private key
label	Capabilities string
Act	Access Token
Ack_1	Acknowledgement
Serv	Service bitstring
Exp	Expiry date
Ts	Time stamp
AGrcode	Authorization grant code
h(x)	hhs value of message x
{x}{k}	Message encrypted with key K

D. Token and Security Policies

The IdP, SP entities and H-SMF are identified, authenticated and use PKI for encryption. However, the details of their message security policies may differ. The ID token may include nonce and nonce keys being associated to entities. To refresh access and ID token, a token request is sent with a grant type of refresh token or the ID token scope when you want to refresh the ID token. If the refresh token is valid, then you get back a new access/refresh token combination with ID token being an option. The token can be revoked by a server by issuing revoke token that includes authorization type, content type, token Id and token type. A federated authorization validation process is performed by the authorization and service servers. The verification of tokens considers a nonce, nonce key, signature, claims, issuer, subject, audience, time stamp and expiry date. While the refresh and revocation use grant type and token ID respectively. For the Data, data name, issuer signature capabilities and expiry date are verified.

IV. Modelling of NS-FId Protocol

We model the proposed protocol using the following entities, UE, SMF, IdP, SPAAA and SS based on the architectural model in [8]. The protocol applies cryptographic primitive in order to provide authentication, confidentiality, integrity, repudiation. The cryptographic primitives used include symmetric and asymmetric encryption, one-way hash function, digital signature and Message Authentication code (MAC). 5G security properties assumptions are based on the specifications in [1]. The UE contains the Universal Subscriber Identity Module (USIM) which has cryptographic capabilities such as key agreement, Key Derivation function (KDF), algorithms, one-way hash function, encryption, MAC facilitated by Elliptic Curve Integrated Encryption Scheme (ECIES) [35].

A. Informal Analysis

The proposed scheme would provide authentication and authorization to UE to access the network services and SSO. It would also omit the need for the optional secondary authentication protocol [1] every time the UE is requesting to access DN services. 5G's emphasis on not sharing the UE's Subscribers Permanent Identifier (SUPI) and other security context outside the HN, is considered in this protocol to enable seamless and secure connectivity when accessing services provisioned by the MNOs or 3P-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. There should also be a stronger linkage between the user and their identities to enforce accountability and non-repudiation in 5G. The process involves initiation, authorization grant, identification, authentication, authorization and granting access.

B. Protocol Message Exchange

A concise federated authentication and authorization message exchange flow of NS-Fid is shown in Fig. 2 and notation in Table II, protocol message exchange is explained next:

Phase1: Service Request

```
Msg1.UE→ SMF: ServReq,(SERVNAME,SID)
```

After the primary authentication, the UE request to establish a service session by sending service request message to SMF in the HN, it includes service name and session ID.

```
Msg2.SMF→ UE: RedSp,(SERVNAME, GPSI,SPID)
```

The SMF checks subscription data and security context of the UE with UDM. Check if the targeted SP is internal or external. If external, then SMF retrieves the GPSI that corresponds with the UE SUPI and send it to the UE along with the SPID. SMF redirects the UE to SP for authorization to access the service.

Phase 2: Identification and Authentication

```
Msg3.UE→SPAAA:AuthzReq,({SERVNAME,SID,GPSI}
{PK(SP)})
```

The UE sends authorization request, it includes the session ID, service name, The UE generic ID, GPSI encrypted with PK(SP).

```
Msg4.SPAAA→UE:RedIdP,({AuthzGrant,EID,
KUE3A},{PK(UE)})
```

When the SP receives request in msg3, it retrieves the UE ID and session ID that includes the HN details and checks the UE's HN agreed policies with the SP. Then generate authorization grant code, EID and the session key KU3A for UE and SPAAA. It sends it to the UE encrypted with PK(UE). Then SPAAA redirects UE to IDP for FID and authentication, hence initiating federated authentication process.

```
Msg5.UE→IDP:IDTokenReq,({AuthzGrant,R1,
GPSI}{PK(IDP)})
```

When the UE receives msg4 it retrieves the K(U3A), then send authorization grant code and a nonce to IDP for FID and IDToken encrypted with the PK(IDP).

```
Msg6.IDP→UE:IDTokenResp,({FID,IDToken,
{hash(IDToken),SKIDP},R1,{hash(IDToken,
{hash(IDToken),SKIDP},R1),SKIDP}}{PKUE})
```

When the IdP receives msg5, it checks the authorization grant code, if there is a need of secondary authentication or use the security context passed over by the SP. It verifies the UE and generates the FID and IDToken. It maps FID with EID and GPSI, the UE profile with MNO/SP attributes providing SSO then sends IDToken response message the includes the ID token, hash of the IDToken, R1, the hash of the whole message and encrypts the whole message with PK(UE). Both hashes are signed with SK(IDP).

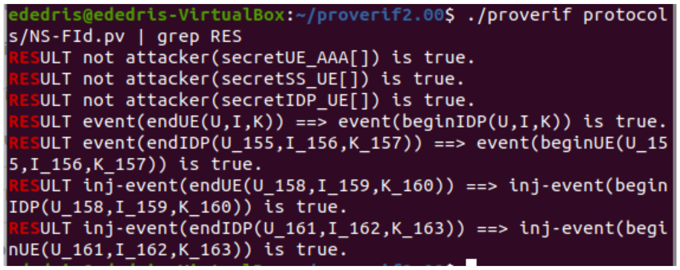
Phase 3: Authorization

```
Msg7.UE→SPAAA:AccessReq,({IDToken,
{hash(IDToken),SKIDP}}{KUE3A})
```

When the UE receives msg6, it retrieves the FID, send access request message to SPAAA for Access/refresh tokens. The message includes the IDToken encrypted with K(UE3A).

```
Msg8.SPAAA→UE:AccessResp,({{AccessToken,
hash(AccessToken),SKAAA},KUESS,
{hash(AccessToken,{hash(AccessToken)
,SKAAA},KUESS),SKAAA}}{KUE3A})
```

When the SPAAA receives, msg7, It verifies the IDToken, checks ID is valid with right parameters, if it doesn't then it issues the access/fresh tokens to the UE. It sends an access



```
ededris@ededris-VirtualBox:~/proverif2.00$ ./proverif protocol
s/NS-FId.pv | grep RES
RESULT not attacker(secretUE_AAA[]) is true.
RESULT not attacker(secretSS_UE[]) is true.
RESULT not attacker(secretIDP_UE[]) is true.
RESULT event(endUE(U,I,K)) ==> event(beginIDP(U,I,K)) is true.
RESULT event(endIDP(U_155,I_156,K_157)) ==> event(beginUE(U_15
5,I_156,K_157)) is true.
RESULT inj-event(endUE(U_158,I_159,K_160)) ==> inj-event(begin
IDP(U_158,I_159,K_160)) is true.
RESULT inj-event(endIDP(U_161,I_162,K_163)) ==> inj-event(begi
nUE(U_161,I_162,K_163)) is true.
```

Fig. 3. 5G NS-FId Protocol ProVerif Result

response message that includes the AccessToken, K(UESS), the access token hash signed with SK(AAA) and encrypted with K(UE3A).

```
Msg9.UE→SS:GrantAccessReq,({AccessToken,
{hash(AccessToken),SKAAA}}{KUESS})
```

When the UE receives msg8, it sends grant access request message that includes AccessToken to SS encrypted with K(UESS).

```
Msg10.SS→UE:GrantAccessResp,
({SERV, hash(SERV),{SK(SS)}}{KUESS})
```

The SS verifies the AccessToken and then sends grant access response, granting UE access to the service.

V. Verification of NS-FId Protocol

A. *Formal Verification*

The modelling of a protocol in ProVerif is composed of declaration, process macros and main processes. The queries are carried out to rectify the correctness and secrecy of a protocol. The ProVerif code is used to specify the protocol concisely using declaration of types, functions, queries and events such as:

```
processUE, free pubChannel:channel,
type key, fun hash(bitstring, bitstring)
: bitstring,
free Secret:bitstring[private]
query attacker(secretUE_SPAAA).
query attacker(secretIDP_UE).
query U: host, SS: host, K: key;
event(endIDP(U, I, K)) ==>
event(beginUE(U, I, K)).
inj-event(endIDP(U, I, K)) ==>
inj-event(beginUE(U, I, K)).
```

B. *Formal Analysis*

We simulated the protocol using unsecure channels and processes:

```
((!procUE())|
(!procSMF())|
(!procIDP())|
(!procSPAAA())|
(!procSS())|
(!keyRegistration))
```

We found no attack on the protocol, on public channel between UE, IDP and SP. The security properties we are interested are the PK(X), SK(X), K(X), mutual authentication, privacy of communication specifically of the FID, IDToken and AccessToken. Using formal analysis, in consideration with adversary vector, there were no attacks on the protocol hence the protocol is secure. ProVerif results in Fig. 3 informs us that the secrecy of Secret, IDToken, AccessToken, FID holds and authentication of UE to IDP and IDP to UE holds as well as implicit authentication of UE to SP in form of non-injective and injective agreements.

The event endIDP means that the IDP has completed the protocol, that the UE received message 6 and sent message 7, event beginIDP means that the IDP sent message 6. These events take as arguments all parameters of the protocol: the AuthzGrant,R1 and EID, IDP which must verify the grant codes and respond to Nonce. If the arguments are true, then IDtoken is sent otherwise it sends either authentication failure for re-authentication initiation. We would like to prove the correspondence below:

```
(*Check authentication of UE to IDP *)
query U: host, I: host, K: pkey;
event(endUE(U, I, K)) ==>
event(beginIDP(U, I, K)).
query U: host, I: host, K: pkey;
inj-event(endUE(U, I, K)) ==>
inj-event(beginIDP(U, I, K)).
(*Check authentication of IDP to UE*)
query U: host, I: host, K: pkey;
event(endIDP(U, I, K)) ==>
 event(beginUE(U, I, K)).
inj-event(endIDP(U, I, K)) ==>
inj-event(beginUE(U, I, K)).
```

The direct proof of this correspondence in ProVerif holds because msg5 is sent before msg6. We also try to prove the correspondence and conclude the desired correspondence by noticing that event which has IDToken as argument cannot be executed before AuthzGrant,R1 and EID, has been sent, that is, before IDToken request has been executed with IDToken Response generating the FID. Which holds in ProVerif with True.

VI. Security Analysis

A. *Protocol Analysis*

The analysis of the protocol is based on security requirements of the protocol based on the security properties of sets 1 [33] and 2 [34]. The analysis based on Set 1 is as follows:

- Secrecy: This is achieved since the EID, FID, K(UE3A) and K(UESS) are never revealed to the attacker. By achieving this property also covers confidentiality and privacy of the protocol data.
- Aliveness: The SP obtain the aliveness of UE when UE send an authorization request to SP with SPID, then SP and HN gets non-injective agreement on FID with the IdP.

- Weak Agreement: This is achieved when HN achieves non-injective agreement on FID with IdP. Also, the HN achieves weak agreement with SP after the session key confirmation with UE.
- Non-injective Agreement: The UE obtains non-injective agreement on FID with the IdP. Also, SP get non-injective agreement on GPSI with HN. Moreover, since FID is a federated ID, an agreement on FID is an agreement with HN and SP. The SP achieves non-injective agreement on EID with the HN after FID is generated by IdP. HN gets non-injective agreement on IDToken and AccessToken with IdP and SP respectively since they include the FID. Which is central to protocol's purpose. The IDToken includes Rand, therefore HN obtains the assurance as a non-injective agreement on IDToken from the IdP to UE.
- Injective Agreement: The injective agreement on tokens between the IdP and SS is central to the protocol's purpose. The injective agreement on EID with the SP assures the UE that IDP is known and trusted. The UE obtain an injective agreement on IDToken and AccessToken with the IdP and SP respectively to assure that the sessions with SP were authorized by the HN. At the same time SS is assured that its session with UE was authorized by SP.

The Analysis based on Set 2 is as follows:

- Mutual Entity Authentication: The UE is authenticated to the IdP if FID and IDToken are generated. Since the IDToken is computed using grant code from SP this enforces weak agreement and implicit authentication from SP after a successful authentication and IDToken. In addition, when UE sent GPSI via SMF to SP, then used that compute grant codes which is used to generate FID and IDToken and they proved to hold enforcing this requirement. Moreover, the creation of FID links the HN, IdP and SP which also empathises this requirement.
- Mutual Key Authentication: Since the generation of K(U3A) and K(UESS) is after the IdP authentication and IDToken, it implicitly authenticates the involved session keys.
- Mutual Key Confirmation: The successful authentication of UE by IdP and security context agreement between the HN, SP and IdP ending with generation of grant codes and Tokens enforces this requirement.
- Key Freshness: ProVerif has no function to check key freshness however the SP checks if GPSI is valid and freshness of K(UE3A).The SP also verifies the IDToken which consists of nonce and time stamp hence checking the freshness of K(UESS). While the IdP checks the authorization grant codes if they are valid. Also checks the computation of the session keys is not the results from previous session and cannot be reused in new session. Since K(UE3A is linked to a service session ID, while K(UESS) is linked to an IDToken and FID. Therefore since the secrecy of these keys is not violated, it implies the keys are fresh.
- Unknown-Key Share: The reachability property in ProVerif is used to check aliveness. The entities ID and Key binding prevents this attack. The inclusion of GPSI, EID, SPID and grant code in the authentication process and in the derivation of session keys proves this requirement. Also, KUE3A is only sent to UE after validation of GPS, SPID encrypted with SP PKID, while KUESS is only sent to UE after the verification of IDToken.
- Key Compromise Impersonation Resilience: Since the KUE3A derived after validation of GPSI and service Id and KUESS derived after Validation of IDToken hence they enforce this requirement. Furthermore, knowing one key in a session is not enough to deduce another. Backward secrecy and forward secrecy of keys are possible, no entity or adversary is capable of computing keys in past session or predict feature keys. Obviously, the pubic keys are globally known but the private keys are only known to the owners. However, to compromise the keys, the ECIES, IdP and SPAAA will have to be compromised at the same time. Also compromising the HN during the primary authentication doesn't mean that federated authentication will be compromised due to the swamping GPSI for EID and EID for FID.

B. *Security Consideration*

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 IDs and enforcing federation practice in the HN and EN concurrently. With Generic Bootstrapping Architecture (GBA) protocol specification [36], the UE can 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 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].

With network slices, multi-tier tenancy on the MNO infrastructure and restriction on sharing security context with 3P, IAM solutions that facilitates FId based protocols need to be considered. In terms of network and service access, end user's authentication should provide SSO in heterogeneous network like 5G. The use of federation relationships between domains should be used for seamless authentication and authorization to a variety of services. 5G should address security with unified multi-level security solutions using abstraction frameworks in press [37] as each level of the network and application have different security requirements and can be complimented by NS-Fid protocol. Our proposed protocol provides mutual authentication, authorization, identity protection, secure access, interoperability and SSO. The implementation of NS-Fid protocol with mobile network can become part mobile network business model for implementing secure service authorization and prevent identity security breaches in networks.

VII. Conclusion

5G promises to provide seamless connectivity and support proximity services for mobile users via wireless access as well as enabling new network and service functions. It will create new use-cases and connect vertical industries which require robust and interoperable security mechanism. In this paper, we explore how FId can be used to provide a universal ID in 5G and other heterogeneous networks. We present a federated network access model that complements the 5G and SBA. We propose a federated protocol NS-FId that can secure the access of service in 5G and SP networks as well as achieving SSO. We model and formally analyse the proposed protocol using formal methods and automated proof verifier ProVerif. We analyse protocol and its security properties based two security properties taxonomies. This protocol could be applied by users to access services and by MNO to share infrastructure resources in any heterogeneous networks like 5G. The future work will be on the integration of the protocol with other use cases in 5G such as D2D communications.

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] 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.

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

[5] VirtuWind, "Deliverable d3.2 detailed intra-domain sdn & nfv architecture," Tech. Rep., 2017.

[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] E. K. K. Edris, M. Aaish, and J. Loo, "The case for federated identity management in 5G communications," in *5th IEEE International Conference on Fog and Mobile Edge Computing (FMEC 2020)*. Paris, France: IEEE, Apr. 2020.

[9] 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.

[10] 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.

[11] R. Xu, Y. Chen, E. Blasch, and G. Chen, "A federated capability-based access control mechanism for internet of things (iots)," in *Sensors and Systems for Space Applications XI*, vol. 10641. International Society for Optics and Photonics, 2018, p. 106410U.

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

[13] 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.

[14] O. Foundation, "Openid foundation — openid," 2007. [Online]. Available: https://openid.net/foundation/

[15] H. Dick, "The oauth 2.0 authorization framework," IETF, Tech. Rep., 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749

[16] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[17] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-based access control*. Artech House, 2003.

[18] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, 2013.

[19] I. Damgård, H. Haagh, and C. Orlandi, "Access control encryption: Enforcing information flow with cryptography," in *Theory of Cryptography Conference*. Springer, 2016, pp. 547–576.

[20] J. B. Dennis and E. C. V. Horn, "Programming semantics for multiprogrammed computations," *Communications of the ACM*, vol. 26, no. 1, pp. 29–35, 1983.

[21] M. Aiash, "A formally verified initial authentication and key agreement protocol in heterogeneous environments using casper/fdr," 2013.

[22] A. Armando, R. Carbone, L. Compagna, J. Cuellar, and L. Tobarra, "Formal analysis of saml 2.0 web browser single sign-on: breaking the saml-based single sign-on for google apps," in *Proceedings of the 6th ACM workshop on Formal methods in security engineering*. ACM, 2008, pp. 1–10.

[23] D. Basin, J. Dreier, L. Hirschi, S. Radomirović, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," 2018, iD: proquest2073641667.

[24] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Drielsma, P. C. Heam, O. Kouchnarenko, J. Mantovani, S. Modersheim, D. V. Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigano, and L. Vigneron, "The avispa tool for the automated validation of internet security protocols and applications," *Computer Aided Verification, Proceedings*, vol. 3576, pp. 281–285, 2005, iD: wos000230755800027.

[25] B. Blanchet, "Modeling and verifying security protocols with the applied pi calculus and proverif," *Found. Trends Priv. Secur.*, vol. 1, no. 1-2, p. 1–135, October 2016. [Online]. Available: https://doi.org/10.1561/3300000004

[26] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 30, no. 2, pp. 198–208, 1983, iD: $gale_ofa$564876.

[27] M. D. Ryan and B. Smyth, "Applied pi calculus," 2011.

[28] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal analysis of 5g eap-tls authentication protocol using proverif," *IEEE Access*, 2020.

[29] K. Bhargavan, C. Fournet, A. D. Gordon, and N. Swamy, "Verified implementations of the information card federated identity-management protocol," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*. ACM, 2008, pp. 123–135.

[30] 3GPP, "System architecture for the 5G system," 3rd Generation Partnership Project, Tech. Rep., 2018.

[31] 3GPP, "5G system; technical realization of service based architecture," Tech. Rep., 2019.

[32] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[33] G. Lowe, "A hierarchy of authentication specifications," pp. 31–43, 1997, $iD : ieee_s$596782.

[34] A. J. A. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. Boca Raton, Fla. ;: CRC, 2001, includes bibliographical references and index.; ID: alma991001301199704781.

[35] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*. Springer, 1985, pp. 417–426.

[36] 3GPP, "Generic bootstrapping architecture (GBA)," Tech. Rep., 2018.

[37] 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, 2019.