INHERITING ENTERPRISE VULNERABILITIES INTO 5G

Highlighting potential need for granular level checks using "Additional scope" under the OAuth2.0 Token Access.

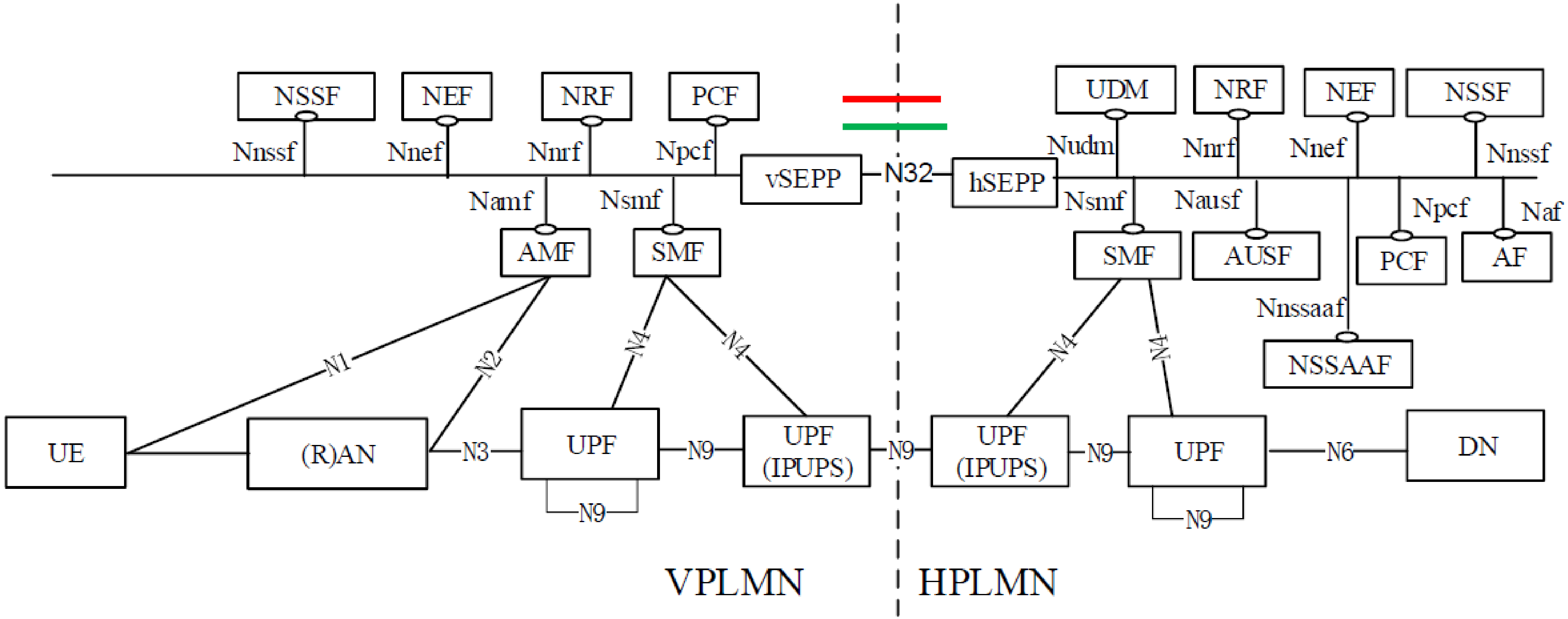
GSMA CVD – 2022-0063

mobileum
Action driven by intelligence

security
intelligence
Mobileum platform

Imran Saleem

The Telco Industry Focus on 5G Security



N32-c

N32-f

N32-c

○ MNO to MNO

○ Handshake, negotiate TLS or PRINS

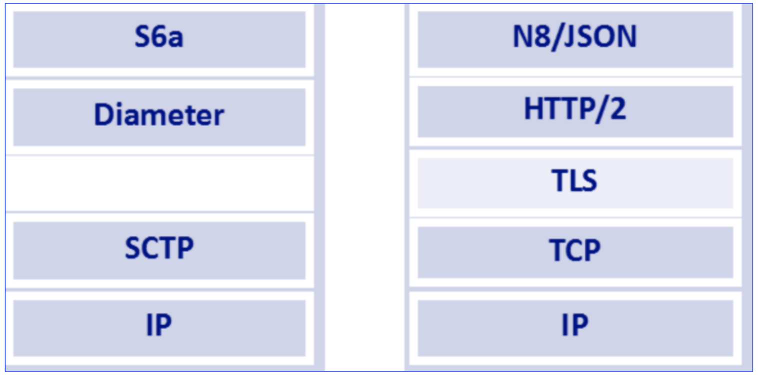
N32-f

○ Delivering the signalling messages

What Telco’s are missing in security!!!

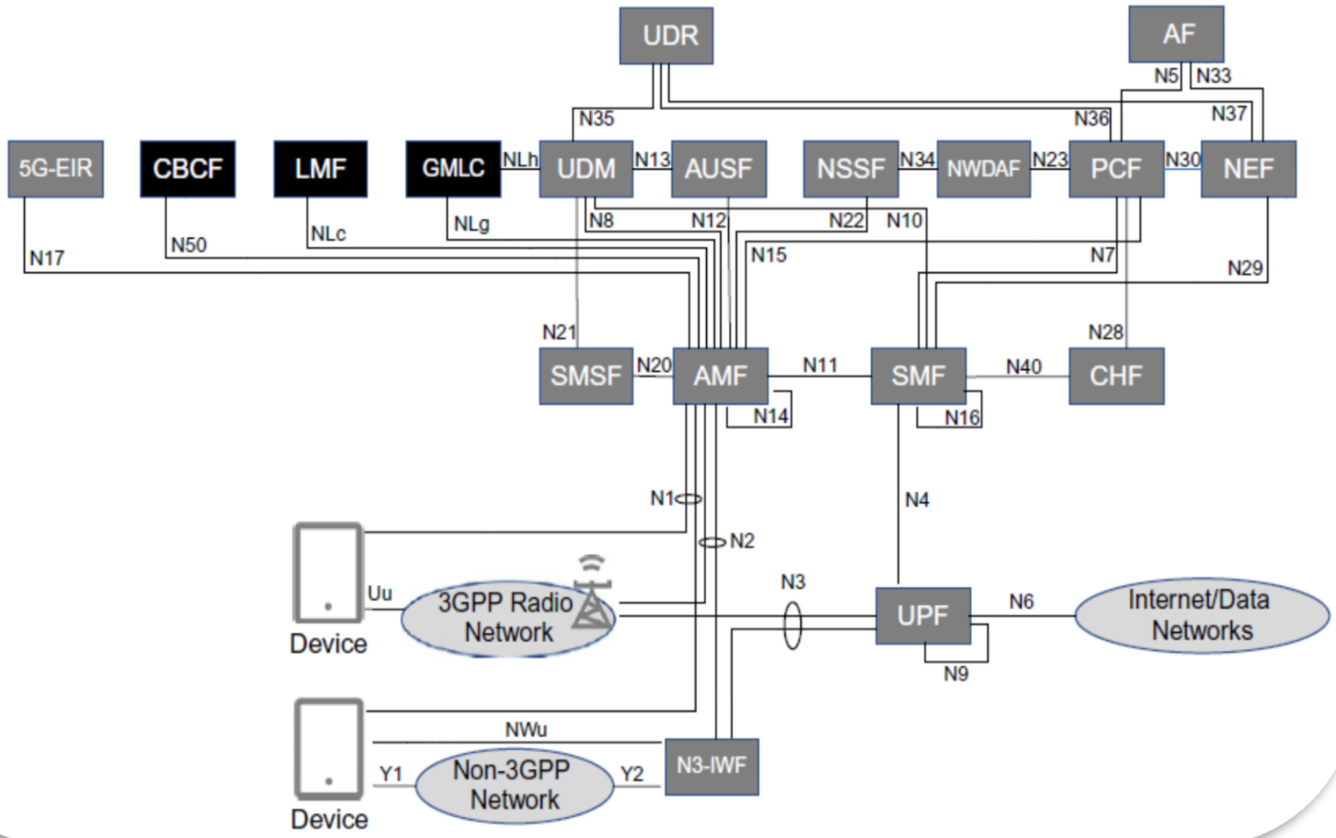
5G has inherited following vulnerabilities from enterprise security

- OWASP API Vulnerabilities
- OAuth2.0 Vulnerabilities
- JSON deserialization attacks.
- JWT Vulnerabilities.
- Various Injections attacks.
- Buffer overflows.



S6a	N8/JSON
Diameter	HTTP/2
	TLS
SCTP	TCP
IP	IP

Talk of the day



Are we ready to adopt the enterprise standards

The presentation talk about one of OAuth2.0 areas that leads to exploit the weakness listed in OWASP API Security.

Focus area:

- OAuth2.0 based Threats.
- OWASP API Security

Outcome:

- Endpoint manipulation for the 5G eco system

Various other OAuth2.0/OWASP weaknesses can impact MNO’s but those are not the topic of discussion today.

- This is a continuous research area.

What is OAuth2.0 Client Credential Grant?

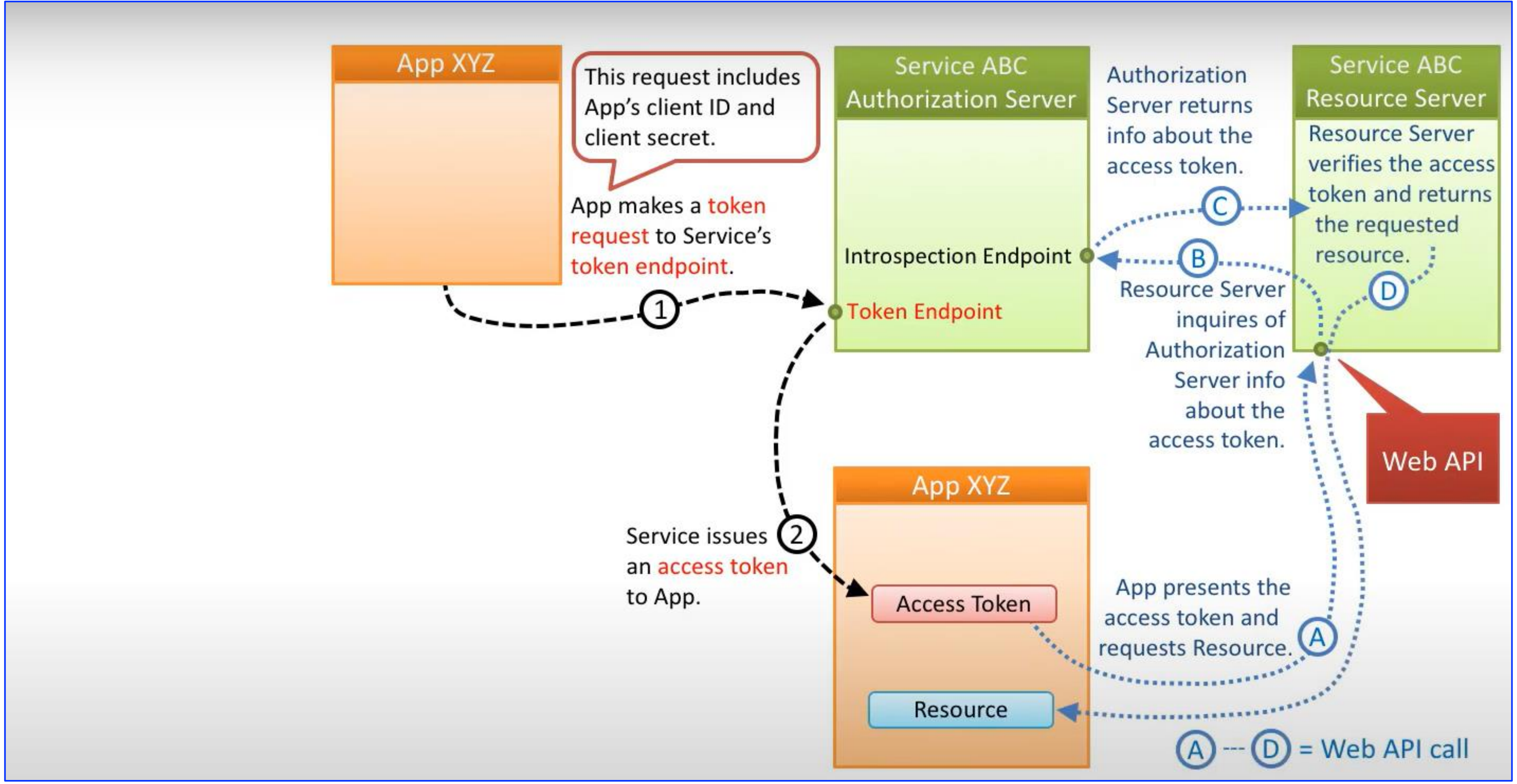
The OAuth 2.0 specification defines a **delegation protocol that provides clients with secure access to the user resources on a service provider.** In a Nutshell OAuth is about how to get a token and how to use a token.

Client Credential type of **grant** is commonly used for server-to-server interactions that must run in the background without immediate interaction with a user.

OAuth2.0 Client
NF Consumer

OAuth2.0 Auth Server
NRF

OAuth2.0 Resource Server
NF producer



This request includes App's client ID and client secret.

App makes a token request to Service's token endpoint.

Service issues an access token to App.

Authorization Server returns info about the access token.

Resource Server verifies the access token and returns the requested resource.

Resource Server inquires of Authorization Server info about the access token.

App presents the access token and requests Resource.

Ⓐ --- Ⓓ = Web API call

OAuth2.0 in IETF

IETF RFC 6749

Section 4.4.2 The "scope" of the access request as described by section 3.3 is "OPTIONAL".

- If the OAuth2.0 client omits the scope parameter when requesting authorization, the authorization server MUST either process the request using a pre-defined default value or fail the request indicating an invalid scope.
- The authorization server SHOULD document its scope requirements and default value (if defined).

“Scope”

Scopes are the OAuth way to explicitly manage the power associated with an access token. A scope can be controlled by the authorization server and/or the end user in order to limit access to resources for OAuth clients that these parties deem less secure or trustworthy.

OAuth2.0 in 3GPP

3GPP TS.29.510 5.4.2.2 (NRF Service)

The "scope" parameter indicating the names of the NF Services that the NF Service Consumer is trying to access (i.e., the expected NF service names);

"The specification doesn't explicitly mention how detailed the "scope" should be and has "optional" attributes that are part of the power associated with the token.

3GPP TS.33.501 14.3.2 Security Architecture

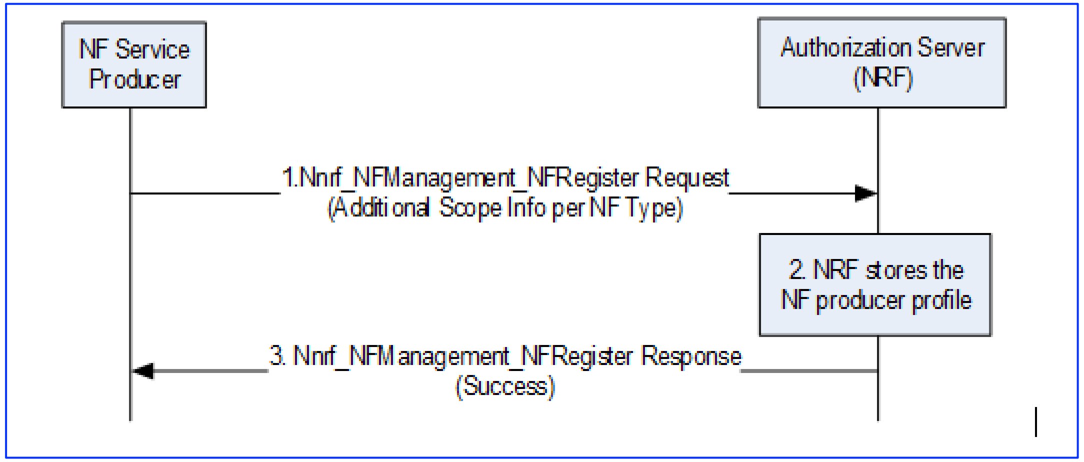
Inputs, Required: the NF Instance Id of the NF Service Consumer, the requested "scope" including the expected NF service name(s).

Again, the spec's doesn't explicitly mentions how detailed the "scope" should be and has left that on the discretion of the MNO for the implementation of "optional" that are part of the power associated with the token.

The OAuth2.0 perspective (IETF V/S 3GPP)

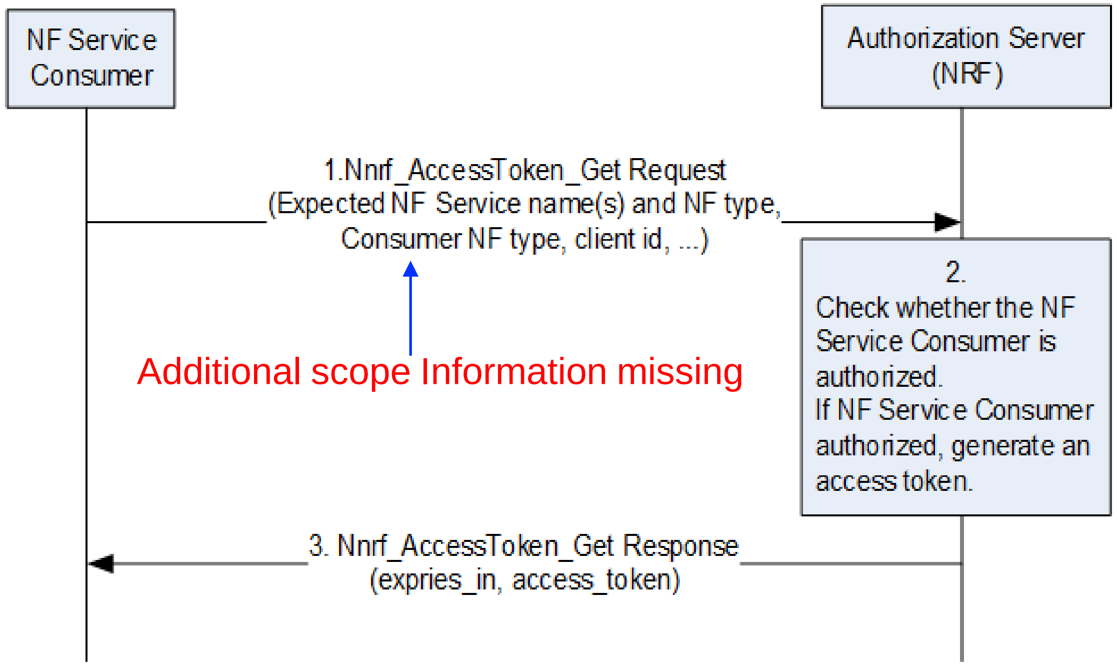
TS 33.501 13.4 Authorization of NF service access

The NF Service Producer, as part of its NF profile, may include "additional scope" information related to the allowed service operations and resources per NF Service Consumer type.


NF Service Producer
Authorization Server (NRF)
1.Nnrf_NFManagement_NFRegister Request (Additional Scope Info per NF Type)
2. NRF stores the NF producer profile
3. Nnrf_NFManagement_NFRegister Response (Success)

3GPP does not mandate the resource name, scope level access per NF consumer and left at the discretion of the MNO to create one.

NRF registration with limited “scope” information



NF Service Consumer

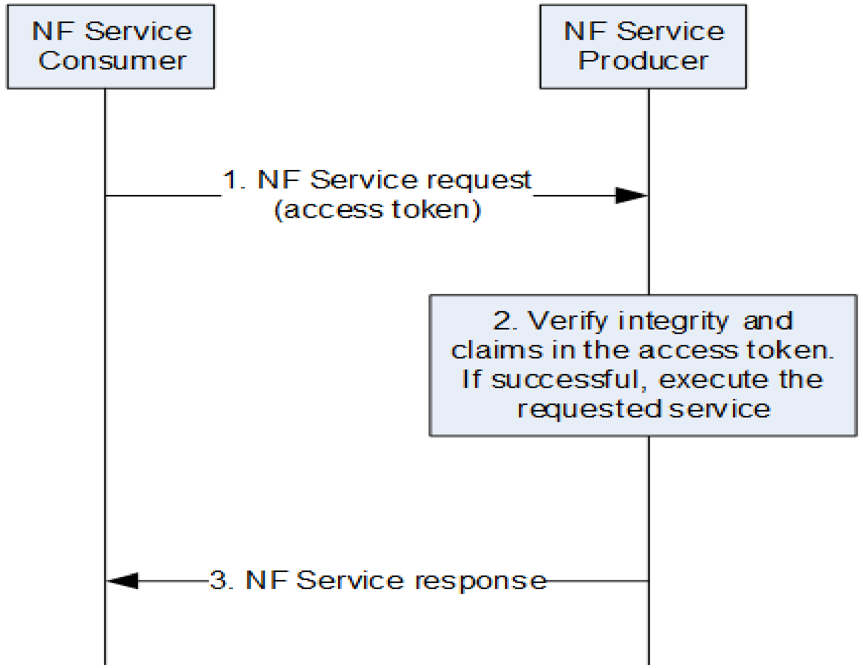
Authorization Server (NRF)

1.Nnrf_AccessToken_Get Request (Expected NF Service name(s) and NF type, Consumer NF type, client id, ...)

Additional scope Information missing

2. Check whether the NF Service Consumer is authorized. If NF Service Consumer authorized, generate an access token.

3. Nnrf_AccessToken_Get Response (expries_in, access_token)



NF Service Consumer

NF Service Producer

1. NF Service request (access token)

2. Verify integrity and claims in the access token. If successful, execute the requested service

3. NF Service response

The OAuth2.0 Token I.E

Reference	Service API	paths	operation type	Request or Response	IE Location	IE Path
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	grant_type
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	nfInstanceId
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	nfType
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetNfType
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	scope
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetNfInstanceId
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	requesterPlmn/mcc
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	requesterPlmn/mnc
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetPlmn/mcc
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetPlmn/mnc
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetSnssaiList/*/sst
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetSnssaiList/*/sd
TS29510_Nnrf_AccessToken.yaml	/oauth2/token	/oauth2/token	post	Request	Body	targetNsiList/*

Registration of the NF Services

```
JavaScript Object Notation: application/json
  Object
    Member Key: ipv4Addresses
    Member Key: nfInstanceId
    Member Key: nfServices
      Array
        Object
          Member Key: apiPrefix
          Member Key: ipEndPoints
          Member Key: nfServiceStatus
          Member Key: scheme
          Member Key: serviceInstanceId
          Member Key: serviceName
            String value: nudm-sdm
            Key: serviceName
          Member Key: versions
        Object
          Member Key: apiPrefix
          Member Key: ipEndPoints
          Member Key: nfServiceStatus
          Member Key: scheme
          Member Key: serviceInstanceId
          Member Key: serviceName
            String value: nudm-uecm
            Key: serviceName
          Member Key: versions
        Object
          Member Key: apiPrefix
          Member Key: ipEndPoints
          Member Key: nfServiceStatus
          Member Key: scheme
          Member Key: serviceInstanceId
          Member Key: serviceName
            String value: nudm-ueau
            Key: serviceName
          Member Key: versions
        Object
```

```
Member Key: apiPrefix
          Member Key: ipEndPoints
          Member Key: nfServiceStatus
          Member Key: scheme
          Member Key: serviceInstanceId
          Member Key: serviceName
            String value: nudm-ee
            Key: serviceName
          Member Key: versions
        Object
          Member Key: apiPrefix
          Member Key: ipEndPoints
          Member Key: nfServiceStatus
          Member Key: scheme
          Member Key: serviceInstanceId
          Member Key: serviceName
            String value: nudm-pp
            Key: serviceName
          Member Key: versions
      Key: nfServices
    Member Key: nfStatus
    Member Key: nfType
    Member Key: plmnList
    Member Key: udmInfo
```

Example of UDM registering its available scopes with information on "additional scope" kept optional.

- Scope is limited to NF Service name being registered with the NRF with missing information on additional scopes.
- If no details on resource name and scope level access is provided then the API end point can be manipulated..

Functional Impact on 5G Ecosystem

This is functional change on the SBA architecture with several business areas of the 5G Ecosystem being exposed.

Speaking of few of them are listed below with its respective exploitation technique.

- Interconnect.

Excessive Data Exposure:

Excessive data exposure via N27 interface.

- Internal services.

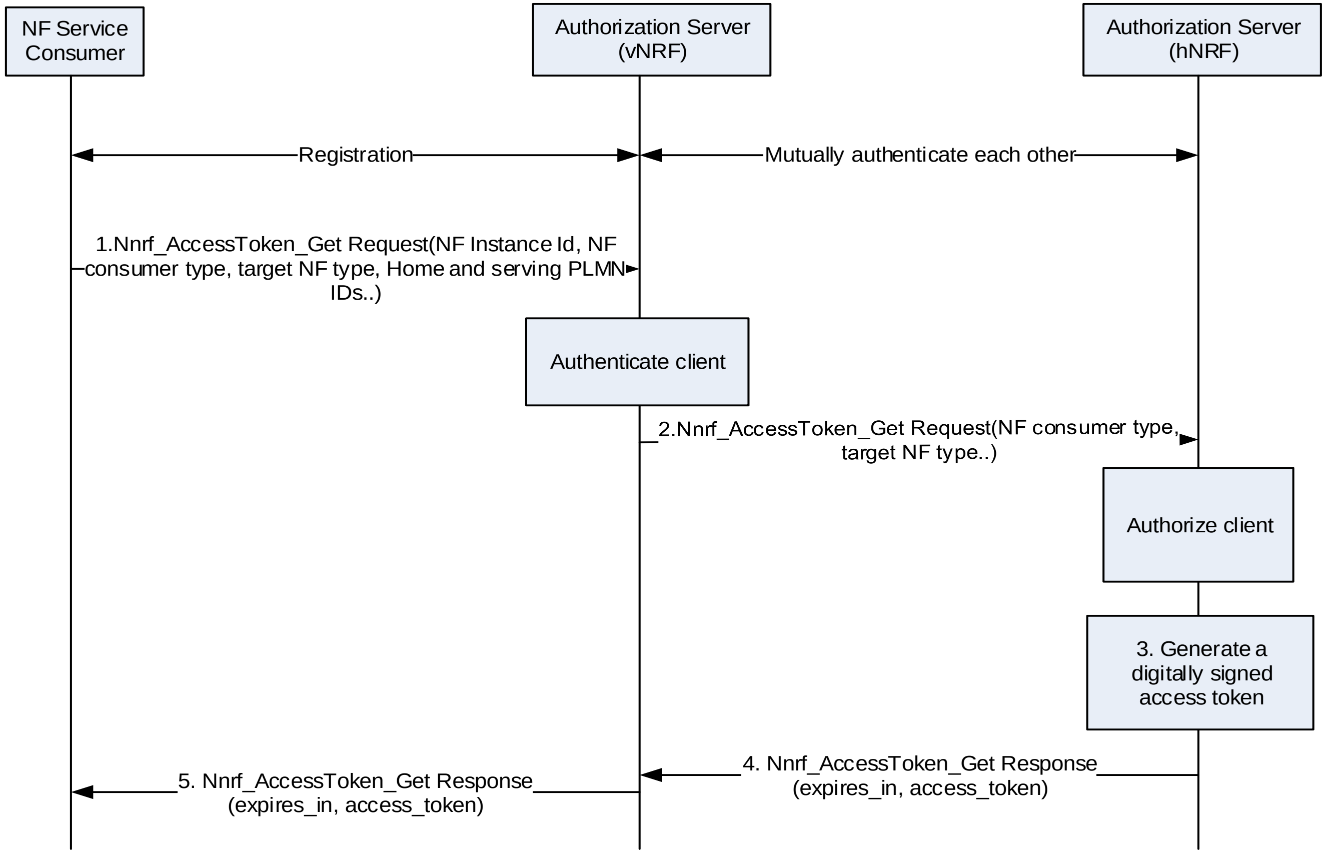
Excessive Data Exposure :

nudm-sdm over privileged service access to SMF and AMF via N8 and N10 interface.

Other functional areas of the 5G business i.e Application & Exposure functions , Network and resource management functions are also exposed to this weakness.

Excessive Data Exposure – N27 Interface- Setting the stage

- The attackers can build multiple use cases to inflict damage to an organization of varying severities.
- The one-use case which is discussed in the paper is not restricting the scope details between vNRF and hNRF via N27 interface which tend to expose more network and service level information thus used to execute further attacks.
- Although this is one out of many interfaces that falls under roaming category.



NF Service Consumer

Authorization Server (vNRF)

Authorization Server (hNRF)

Registration

Mutually authenticate each other

1.Nnrf_AccessToken_Get Request(NF Instance Id, NF consumer type, target NF type, Home and serving PLMN IDs..)

Authenticate client

2.Nnrf_AccessToken_Get Request(NF consumer type, target NF type..)

Authorize client

3. Generate a digitally signed access token

4. Nnrf_AccessToken_Get Response (expires_in, access_token)

5. Nnrf_AccessToken_Get Response (expires_in, access_token)

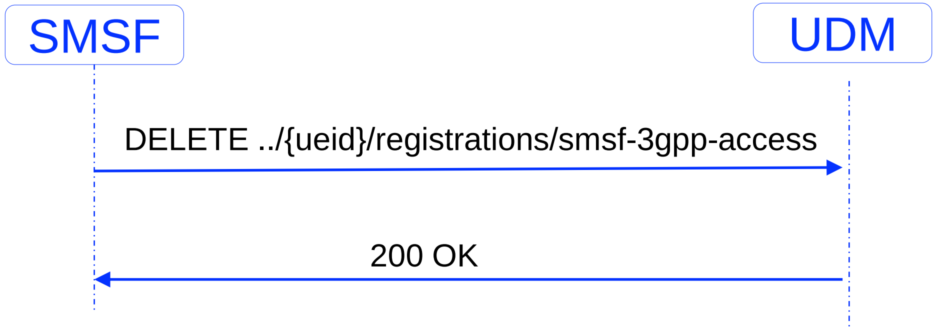
Not restricting the scope details between vNRF and hNRF tend to expose more network level and service level information which can be exploited due to lack of visibility on the OAuth2.0 .

Excessive Data Exposure - (Service Unavailability-DoS)

One of the use case is CAT3 Endpoint’s which can be exploited due to lack of visibility on the OAuth2.0 .

Reference	paths	operation type	operationId	Risk Assessment	Comment
TS29503_Nudm_UECM.yaml	/{ueId}/registrations/smf-registrations/{pduSessionId}	delete	SmfDeregistration	Medium	The SMF sends a DELETE request to the resource representing the individual SMF registration that is to be deregistered.
TS29503_Nudm_UECM.yaml	/{ueId}/registrations/smsf-3gpp-access	delete	3GppSmsfDeregistration	Medium	The SMSF sends a DELETE request to the resource representing the UE's SMSF registration for 3GPP access.
TS29503_Nudm_UECM.yaml	/{ueId}/registrations/smsf-non-3gpp-access	delete	Non3GppSmsfDeregistration	Medium	The SMSF sends a DELETE request to the resource representing the UE's SMSF registration for non 3GPP access.

```
  summary: delete the SMSF registration for 3GPP access
      operationId: 3GppSmsfDeregistration
      tags:
        - SMSF Deregistration for 3GPP Access
parameters:
        - name: ueId
          in: path
          description: Identifier of the UE
          required: true
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        - name: smsf-set-id
          in: query
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/NfSetId'
```



SMSF

UDM

DELETE ../{ueid}/registrations/smsf-3gpp-access

200 OK

- *service unavailability by the use of “delete” method for various NF services.*
- *UDM exposing unwanted endpoint can be exploited due to improper access controls.*

Highlighting potential need for granular level checks using "Additional scope" under the OAuth2.0 Token Access.

Highlighting potential need for granular level checks using "Additional scope" under the OAuth2.0 Token Access.

Example:

```
security:
  - {}
  - oAuth2ClientCredentials:
    - nnrf-nfm

paths:
  /nf-instances:
    get:
      security:
        - {}
        - oAuth2ClientCredentials:
          - nnrf-nfm
        - oAuth2ClientCredentials:
          - nnrf-nfm
          - nnrf-nfm:nf-instances:read
      parameters:
      (...)
      responses:
      (...)

components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nnrf-nfm: Access to the Nnrf_NFManagement API
            nnrf-nfm:nf-instances:read: Read access to the NF Instances (Collection) resource
```

NF service name (Scope) : Nnrf_NFManagement

resource name (optional) : GetNFInstances

resource/operation-level scopes (optional) : get/post/put/delete

invoke a specific operation on a specific resource.

Remedial Steps.

- This is functional change on the SBA architecture.
- 3GPP should investigate "additional scope" and whether OAuth2.0 procedures can be made stricter and use of “additional scope” are mandated and not left optional.
- This will ensure areas that are left open in the OAuth2.0 IETF RFC 6749 are handled in the 3GPP specifications.
- Build predefined/desired communication matrix with set of parameters among NF services/Instances/Interfaces.
- NF to offer its services to only predefined list of consumers marked during the NRF registration.
- Prevent consumer NFs from receiving more data than they require.

THANK YOU

mobileum

Action driven by intelligence