**3GPP TSG-SA3 Meeting #** **105e *S3-214493***

**e-meeting, 8 - 19 November 2021** Revision of S3-214094

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **Draft CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Security aspects of eNA | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China mobile, Huawei, Hisilicon, Nokia, Nokia Shanghai Bell, Lenovo, Motorola Mobility, Ericsson, Mavenir, Verizon | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 930007 | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Security aspects for eNA need to be specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Enhancements to 5GS on the security aspects for eNA. Specifically:  - Authorization of NF Service Consumers for data access via DCCF  - Authorization of NF Service Consumers for data access via DCCF when notification sent via MFAF  - Security protection of data via Messaging Framework  - Protection of data transferred between AF and NWDAF  - Protection of UE data in transit between NFs  Change history of the living document:  SA3#104-e Ad-hoc:   * S3-213614 * S3-213618 * S3-213717 * S3-213718 * S3-213719   SA3#105-e:   * S3-214303 * S3-214513 * S3-214514 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Enhanced support of eNA will not have necessary security aspects specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 13.4.1.1.2, Annex X.1 (new), Annex X.2 (new), Annex X.3 (new), Annex X.4 (new), Annex X.5 (new), Annex X.6 (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[12] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[25] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"

[26] Void

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

[38] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

[60] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[61] IETF RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] Internet draft draft-ietf-emu-rfc5448bis: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS with TLS 1.3"

[77] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] RFC 2818: "HTTP Over TLS".

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[xx] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

\*\*\* NEXT CHANGE \*\*\*

Annex X (normative):  
Security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2

X.1 General

This Annex provides security requirements and procedures for the Network Automation features.

The feature for enablers for Network Automation by 5GS is described in 3GPP TS23.501[2] and 3GPP TS23.288 [xx].

X.2 Authorization of NF Service Consumers for data access via DCCF

The detailed procedure for NF Service Consumer to receive data from Service Producers via DCCF is depicted in Figure X.2-1:



Figure X.2-1: Service Consumer Authorization to receive data from Service Producers via DCCF

1-3. NF Service Consumer shall send a request to the NRF to receive an access token to request services of DCCF. NRF after verifying shall generate access token and sends it to the NF Service Consumer.

4. The NF Service Consumer initiates a NF service request to the DCCF which includes the access\_token\_nwdaf. The NF Service Consumer shall also generate a Client Credentials Assertion (CCA) token (CCA\_NWDAF) as described in the clause 13.3.8 and include it in the request message in order to authenticate itself towards the NF Service Producers.

NOTE: The procedure of NF Service Consumer (e.g. NWDAF) requesting the services provided by NF Service Producer via DCCF is defined in Clause 6.2.6.3 of TS 23.288[x].

5. The DCCF shall verify if the access\_token\_nwdaf is valid and executes the service.

6. The DCCF determines the NF Service Producer(s) from where the data is to be collected (as specified in Clause 6.2.6.3.2 in TS 23.288[x]).

NOTE: If the NF Service Consumer sends the NF Service Producer information (i.e. NF Service Producer type and Instance ID) along with the service request in Step 4, then DCCF does not determine the NF Service Producer, but requests an access token from the NRF using the NF Producer details sent by the NF Service Consumer (as described in Step 7.)

7. The DCCF sends a Nnrf\_AccessToken\_Get request to NRF including the information to identify the target NF (NF Service Producer), the source NF (NF Service Consumer e.g. NWDAF), the NF Instance ID of DCCF and the CCA\_NWDAF provided by the NF Service Consumer.

NOTE: The NF Instance ID of DCCF is included in a different IE than source NF so that Rel-16 NRF will ignore the new IE.

8. The NRF shall check whether the DCCF and the NF Service Consumer (e.g. NWDAF) are allowed to access the service provided by the identified NF Service Producers. NRF authenticates both DCCF and NWDAF based on one of the SBA methods described in clause 13.3.1.2. DCCF may include an additional CCA for authentication.

NOTE: Rel-16 NRF takes CCA to authenticate NF Service Consumer if available (i.e., authentication is not based on TLS).

NOTE: In the case the NRF is from Rel-16 or earlier, after the NRF receives Nnrf\_AccessToken\_Get request, the NRF validates whether the NF Service Consumer (e.g., NWDAF) is authorized to receive the requested service from the NF Service Producer. The NRF from Rel-16 or earlier does not validate whether the DCCF is authorized to receive the requested service.

9. The NRF after successful verification then generates and provides an access token to the DCCF as described in the clause 13.4.1.1.2, with NF Service Consumer Instance (subject), and an additional access token claim containing the identity of DCCF, in order to authorize both NF Service Consumer (i.e. NWDAF) and DCCF to consume the services of NF Service Producer.

NOTE: In the case the NRF is from Rel-16 or earlier, the NRF generates an OAuth2.0 access token with “subject” claim mapped to the NF Service Consumer (e.g., NWDAF) and no additional claim for the DCCF identity is added.

10. The DCCF requests service from the NF Service Producer. The request also consists of CCA\_NWDAF, so that the NF Service Producer(s) authenticates the NF Service Consumer (e.g. NWDAF).

11. The NF Service Producer(s) authenticate the NF Service Consumer and verify the access token as specified in the Clause 13.4.1.1.2 and ensures that the DCCF identity is included as an access token additional claim. If the DCCF identity is not included in the access token additional claims, e.g., NRF is Release 16 or prior, the NF Service Producer shall authorize the DCCF locally. After authentication and authorization is successful, the NF Service Producer(s) execute the service after successful verification. DCCF may include an additional CCA for authentication.

NOTE: Rel-16 NF Service Producer takes CCA to authenticate NF Service Consumer if available (i.e., authentication is not based on TLS).

12. The NF Service Producer(s) shall provide requested data to the DCCF.

13. The DCCF forwards the received data to the data consumer(s).

NOTE: In the case a new data consumer comes at a later stage to request the data, which is already being collected by DCCF, steps 1-10 apply. When the request is received by the NF Service Producer (i.e. the data producer), it authenticates the NF Service Consumer and verifies the access token provided along with the service request and sends to DCCF the access token verification response. DCCF based upon the response received, either updates the subscription info to include the new data consumer as well and sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288[x]), or in the case of access token verification failure, the DCCF rejects the request received by the data consumer.

NOTE: In the case the NF Service Producer is from Rel 16 or earlier, the NF Service Producer authorizes the NF Service Consumer (e.g., NWDAF) by validating the received OAuth2.0 access token which has the “subject” claim maps to the NF Service Consumer (e.g., NWDAF). Rel-16 or earlier NF Service Producer authorization of the DCCF is a deployment specific based on any of the available 5GC authorization method(s).

X.3 Authorization of NF Service Consumers for data access via DCCF when notification sent via MFAF

The detailed procedure for NF Service Consumer to receive data from Service Producers via DCCF when notification is sent via MFAF is depicted in Figure X.3-1:



Figure X.3-1: Service Consumer Authorization to receive data from Service Producers via MFAF

Steps 1-9 are same as Steps 1 – 9 of Annex X.2

10-11. The DCCF sends an access token request to the NRF to request service from MFAF. NRF after verifying sends access\_token\_dccf to DCCF to consume the services of MFAF.

12. DCCF shall then send the Nmfaf\_3daDataManagement\_Configure request to MFAF (as specified in the Clause 6.2.6.3.2 in TS 23.288) along with the access\_token\_dccf.

Steps 13 – 14 are same as Steps 10 – 11 of Annex X.2

15. The NF Service Producer(s) shall provide requested data to the MFAF.

16. The MFAF forwards the received data to the data consumer(s).

NOTE: In the case a new data consumer comes at a later stage to request the data, which is already being collected by DCCF, steps 1-9 apply. When the request is received by the NF Service Producer (i.e. the data producer), it authenticates the NF Service Consumer and verifies the access token provided along with the service request and sends to DCCF the access token verification response. DCCF based upon the response received, either updates the subscription info at the MFAF to include the new data consumer as well and MFAF sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288[x]), or in the case of access token verification failure, the DCCF rejects the request received by the data consumer and does not update the subscription at the MFAF.

NOTE: In the case the NF Service Producer is from Rel 16 or earlier, the NF Service Producer authorizes the NF Service Consumer (e.g., NWDAF) by validating the received OAuth2.0 access token which has the “subject” claim maps to the NF Service Consumer (e.g., NWDAF). Rel-16 or earlier NF Service Producer authorization of the DCCF is a deployment specific based on any of the available 5GC authorization method(s).

X.4 Security protection of data via Messaging Framework

The transfer of the data between the data source and data consumer via the messaging framework shall be confidentiality, integrity, and replay protected.

Confidentiality protection, integrity protection, and replay-protection shall be supported on the new interfaces between 3GPP entities and MFAF by reusing the existing security mechanism defined for SBA in TS 33.501 Clause 13.

X.5 Protection of data transferred between AF and NWDAF

As specified in TS 23.288[xx], the NWDAF may interact with an AF to collect data from UE Application(s) as an input for analytics generation. The AF can be in the MNO domain or an AF external to MNO domain. To enhance the 5GS to support collection and utilisation of UE related data for providing the inputs to generate analytics information (to be consumed by other NFs), the communication between AF and NWDAF needs to be secured.

The NWDAF interacts with the 5GC NFs and the AF using Service-based Interfaces. The existing 5G security mechanism can be reused for the transfer of UE data over the SBA interface between AF and NWDAF. When the AF is located in the operator’s network, the NWDAF uses Service-Based Interface as depicted in clause 13 to communicate with the AF directly. When the AF is located outside the operator’s network, the NEF is used to exchange the messages between the AF and the NWDAF. The security aspects of NEF is specified in clause 12.

X.6 Protection of UE data in transit between NFs

According to clause 13.1.0, all network functions shall support mutually authenticated TLS and HTTPS. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. Thus, communication between NFs is integrity, confidentiality and replay protected.

NFs shall obtain an access token from NRF for requesting analytics from an analytics function or providing analytics data to the analytics function.

\*\*\* NEXT CHANGE \*\*\*

##### 13.4.1.1.2 Service Request Process

The complete service request is a two-step process including requesting an access token by NF Service Consumer (Step 1, i.e. 1a or 1b), and then verification of the access token by NF Service Producer (Step 2).

NOTE: The service request process regarding the enabler for network automation is specified in Annex X.

**Step 1: Access token request**

Pre-requisite:

- The NF Service consumer (OAuth2.0 client) is registered with the NRF (Authorization Server).

- The NF Service Producer (OAuth2.0 resource server) is registered with the NRF (Authorization Server) with "additional scope" information per NF type.

- The NRF and NF Service Producer share the required credentials.

- The NRF and NF have mutually authenticated each other.

**1a. Access token request** **for** **accessing services of NF Service Producers of a specific NF type**

The following procedure describes how the NF Service Consumer obtains an access token before service access to NF Service Producers of a specific NF type.



Figure 13.4.1.1.2-1: NF Service Consumer obtaining access token before NF Service access

1. The NF Service Consumer shall request an access token from the NRF in the same PLMN using the Nnrf\_AccessToken\_Get request operation. The message shall include the NF Instance Id(s) of the NF Service Consumer, the requested "scope" including the expected NF Service name(s) and optionally "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), NF type of the expected NF Service Producer instance and NF Service Consumer. The NF Service Consumer may also include a list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances.

The message may include the NF Set ID of the expected NF Service Producer instances.

The message may include a list of S-NSSAIs of the NF Service Consumer.

2. The NRF may verify that the input parameters (e.g., NF type) in the access token request match with the corresponding ones in the public key certificate of the NF Service Consumer or those in the NF profile of the NF Service Consumer. The NRF checks whether the NF Service Consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the NRF shall then generate an access token with appropriate claims included. The NRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45]. If the NF Service Consumer is not authorized, the NRF shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer (subject), NF type of the NF Service Producer (audience), expected service name(s), (scope), expiration time (expiration) and optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources). The claims may include a list of NSSAIs or NSI IDs for the expected NF Service Producer instances. The claims may include the NF Set ID of the expected NF Service Producer instances.

3. If the authorization is successful, the NRF shall send access token to the NF Service Consumer in the Nnrf\_AccessToken\_Get response operation, otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43]. The other parameters (e.g., the expiration time, allowed scope) sent by NRF in addition to the access token are described in TS 29.510 [68].

The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Service Producer NF type listed in claims (scope, audience) during their validity time.

**1b. Access token request for accessing services of a specific NF Service Producer instance / NF Service Producer service instance**

The following steps describes how the NF Service Consumer obtains an access token before service access to a specific NF Service Producer instance / NF Service Producer service instance. 1. The NF Service Consumer shall request an access token from the NRF for a specific NF Service Producer instance / NF Service Producer service instance. The request shall include the NF Instance Id(s) of the requested NF Service Producer, the expected NF Service name, optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources) and NF Instance Id of the NF Service Consumer.

2.The NRF checks whether the NF Service Consumer is authorized to use the requested NF Service Producer instance/NF Service Producer service instance, and then proceeds to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer (subject), NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer (audience), expected service name(s) (scope), optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources), and expiration time (expiration).

3. The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NF Service Consumer. The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer instance listed in claims (scope, audience) during their validity time.

**Step 2: Service access request based on token verification**

The following figure and procedure describe how authorization is performed during Service request of the NF Service Consumer. Prior to the request, the NF Service Consumer may perform Nnrf\_NFDiscovery\_Request operation with the requested additional scopes to select a suitable NF Service Producer (resource server) which is able to authorize the Service Access request.



Figure 13.4.1.1.2-2: NF Service Consumer requesting service access with an access token

Pre-requisite: The NF Service Consumer is in possession of a valid access token before requesting service access from the NF Service Producer.

1. The NF Service Consumer requests service from the NF Service Producer. The NF Service Consumer shall include the access token.

The NF Service Consumer and NF Service Producer shall authenticate each other following clause 13.3.

2. The NF Service Producer shall verify the token as follows:

- The NF Service Producer ensures the integrity of the token by verifying the signature using NRF’s public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service Producer shall verify the claims in the token as follows:

NOTE: Void.

- It checks that the audience claim in the access token matches its own identity or the type of NF Service Producer. If a list of NSSAIs or list of NSI IDs is present, the NF Service Producer shall check that it serves the corresponding slice(s).

- If an NF Set ID present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.

- If scope is present, it checks that the scope matches the requested service operation.

- If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.

- It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

- If the CCA is present in the service request, it may verify the CCA as specified in clause 13.3.8.3 and that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token matches the subject claim in the CCA.

3. If the verification is successful, the NF Service Producer shall execute the requested service and responds back to the NF Service Consumer. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43].

\*\*\* END CHANGES \*\*\*