**3GPP TSG-SA3 Meeting #107-e *S3-220698-r2***

**e-meeting, 16 - 20 May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1363** | **rev** | **-** | **Current version:** | **17.05.0** |  |
|  |
| *For* [***HELP***](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:***  | NSWO alignment with SA2 specs |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-05-10 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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 canbe 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:*** | First:As per SA2 LS S2-2203253, NSWO roaming architecture is defined in 23501 section 4.2.15. Therefore, clean up is required in 33501 to avoid duplicate content.Please note, following option is not agreed in SA2 description:*WLAN AN routes AAA messages to the NSWO NF in the VPLMN. The NSWO NF in the VPLMN, acting as a 3GPP AAA proxy, routes the AAA messages to the NSWO NF in the HPLMN*Second: as per TS 23.501, NSWO NF is mentioned NSWOF- Non-Seamless WLAN Offload Function. However, TS 33.501 stills uses NSWO NF. Therefore, alignment is needed for the wording.Third: Following EN needs to be removed as SA2 updated the specificationEditor’s Note: The above text may need to be updated to align with NSWO architecture in TS 23.501. |
|  |  |
| ***Summary of change:*** | Proposing to remove the roaming architecture details in Annex S.4 and add refrence of TS 23501Proposing to rename NSWO NF to NSWOFProposing to remove EN  |
|  |  |
| ***Consequences if not approved:*** | Duplicate and incosistent content in 33501 and 23501 specs  |
|  |  |
| ***Clauses affected:*** | 3.2, Annex S  |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core Network

5G-AN 5G Access Network

5G-RG 5G Residential Gateway

NG-RAN 5G Radio Access Network

5G AV 5G Authentication Vector

5G HE AV 5G Home Environment Authentication Vector

5G NSWO 5G Non-Seamless WLAN Offload

5G SE AV 5G Serving Environment Authentication Vector

ABBAAnti-Bidding down Between Architectures

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

AMF Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF Authentication credential Repository and Processing Function

AUSF Authentication Server Function

AUTN AUthentication TokeN

AV Authentication Vector

AV' transformed Authentication Vector

BAP Backhaul Adaptation Protocol

BH Backhaul

CCA Client Credentials Assertion

Cell-ID Cell Identity as used in TS 38.331 [22]

CH Credentials Holder

CHO Conditional Handover

CIoT Cellular Internet of Things

cIPX consumer's IPX

CKSRVCC Cipher Key for Single Radio Voice Continuity

CP Control Plane

cSEPP consumer's SEPP

CTR Counter (mode)

CU Central Unit

DCS Default Credentials Server

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

EN-DC E-UTRA-NR Dual Connectivity

ENSI External Network Slice Inforamtion

EPS Evolved Packet System

FN-RG Fixed Network RG

gNB NR Node B

GUTI Globally Unique Temporary UE Identity

HRES Hash RESponse

HXRES Hash eXpected RESponse

IAB Integrated Access and Backhaul

IKE Internet Key Exchange

IKSRVCC Integrity Key for Single Radio Voice Continuity

IPUPS Inter-PLMN UP Security

IPX IP exchange service

KSI Key Set Identifier

KSISRVCC Key Set Identifier for Single Radio Voice Continuity

LI Lawful Intercept

MBSF Multicast/Broadcast Service Function

MBSTF Multicast/Broadcast Service Transport Function

MeNB Master eNB

MN Master Node

MO-EDT Mobile Originated Early Data Transmission

MT-EDT Mobile Terminated Early Data Transmission

MR-DC Multi-Radio Dual Connectivity

MSK Master Session Key

N3IWF Non-3GPP access InterWorking Function

NAI Network Access Identifier

NAS Non Access Stratum

NDS Network Domain Security

NEA Encryption Algorithm for 5G

NF Network Function

NG Next Generation

ng-eNB Next Generation Evolved Node-B

ngKSI Key Set Identifier in 5G

N5CW Non-5G-Capable over WLAN

N5GC Non-5G-Capable

NIA Integrity Algorithm for 5G

NR New Radio

NR-DC NR-NR Dual Connectivity

NSSAI Network Slice Selection Assistance Information

NSSAA Network Slice Specific Authentication and Authorization

NSWO Non-Seamless WLAN Offload

NSWOF Non-Seamless WLAN Offload Function

PDN Packet Data Network

PEI Permanent Equipment Identifier

pIPX producer's IPX

PRINS PRotocol for N32 INterconnect Security

pSEPP producer's SEPP

PUR Preconfigured Uplink Resource

QoS Quality of Service

RES RESponse

SCG Secondary Cell Group

SEAF SEcurity Anchor Function

SCP Service Communication Proxy

NOTE: Void. Security Gateway

SEPP Security Edge Protection Proxy

SgNB Secondary gNB

SIDF Subscription Identifier De-concealing Function

SMC Security Mode Command

SMF Session Management Function

SN Secondary Node

SN Id Serving Network Identifier

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TWAP Trusted WLAN Access Point

TWIF Trusted WLAN Interworking Function

TSC Time Sensitive Communication

UE User Equipment

UEA UMTS Encryption Algorithm

UDM Unified Data Management

UDR Unified Data Repository

UIA UMTS Integrity Algorithm

ULR Update Location Request

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module

XRES eXpected RESponse

Annex S (normative):
Support for Non-seamless WLAN offload (NSWO) in 5GS

# S.1 Introduction

Non-seamless WLAN offload (NSWO) is an optional capability of a UE supporting WLAN radio access. A UE supporting non-seamless WLAN offload may, while connected to WLAN access, route specific IP flows via the WLAN access without traversing the 3GPP core network.

The present annex specifies the support for authentication for NSWO in 5GS (5G NSWO).

# S.2 General

5G NSWO shall use EAP-AKA’, as specified in RFC 5448 [12], for authentication. The EAP-AKA’ implementations shall comply with the EAP-AKA’ profile specified in Annex F of the present document.

A new network function, called NSWOF, is introduced to support authentication for NSWO in 5GS. The NSWOF interfaces to the WLAN access network using SWa interface and interfaces to the AUSF using Service Based Interface (SBI).

# S.3 Authentication procedure

## S.3.1 5G NSWO co-existence with EPS NSWO

An HPLMN that supports 5G NWSO and wants the UE to use 5G NSWO shall configure the UE to use 5G NSWO. This configuration shall be either on the USIM or ME, with configuration on the USIM taking precedence over the ME.

A UE that supports 5G NSWO and is configured to use 5G NSWO shall always use 5G NSWO as described in clause S.3.2 (i.e., it shall not use EPS NSWO defined in TS 23.402[97]). Otherwise, the UE may use EPS NSWO (e.g., UE does not support 5G NSWO or not configured to use 5G NSWO).

NOTE: Such a configuration ensures that the UE supporting 5G NSWO cannot be downgraded to use EPS NSWO.

The network may support both 5G NSWO and EPS NSWO. In such a case, the routing of the AAA messages is determined by the network based on the realm part of the UE Identity (e.g., realm contains epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org (EPS NSWO) or 5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org (5G NSWO)). Which entities in the network perform this routing decision is dependent on the network configuration.

## S.3.2 5G NSWO procedures



Figure: S.3-1: Authentication procedure for NSWO in 5GS

1. The UE establishes a WLAN connection between the UE and the WLAN Access Network (AN), using procedures specified in IEEE 802.11[80].

2. The WLAN AN sends an EAP Identity/Request to the UE.

3. The UE sends an EAP Response/Identity message. The UE shall use the SUCI in NAI format (i.e., username@realm format as specified in clause 28.7.3 of TS 23.003[19]) as its identity irrespective of whether SUPI Type configured on the USIM is IMSI or NAI. If the SUPI Type configured on the USIM is IMSI, the UE shall construct the SUCI in NAI format with username containing the encrypted MSIN and the realm part containing the MCC/MNC.

4. The EAP Response/Identity message shall be routed over the SWa interface towards the NSWOF based on the realm part of the SUCI.

NOTE 1: NSWOF acts as SBI/AAA proxy between the AUSF and the WLAN Access Network.

5. The NSWOF shall send the message Nausf\_UEAuthentication\_Authenticate Request with SUCI, Access Network Identity and NSWO indicator towards the AUSF. NSWO\_indicator is used to indicate to the AUSF that the authentication request is for Non-seamless WLAN offload purposes. The NSWOF shall set the Access Network Identity to "5G:NSWO".

6. The AUSF (acting as the EAP authentication server) shall send a Nudm\_UEAuthentication\_Get Request to the UDM, including SUCI and the Access Network Identity and NSWO indicator.

7. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. Based on the NSWO indicator, the UDM/ARPF shall select the EAP-AKA´ authentication method and generate an authentication vector using the Access Network Identity as the KDF input parameter. The UDM shall include the EAP-AKA’ authentication vector (RAND, AUTN, XRES, CK´ and IK´) and may include SUPI to AUSF in a Nudm\_UEAuthentication\_Get Response message.

8. The AUSF shall store XRES for future verification. The AUSF shall send the EAP-Request/AKA'-Challenge message to the NSWOF in a Nausf\_UEAuthentication\_Authenticate Response message.

NOTE: The Access Network Identity is carried in the AT\_KDF\_INPUT attribute in EAP-AKA' as defined in RFC 5448 [12].

9. The NSWF shall send the EAP-Request/AKA'-Challenge message to the WLAN AN over the SWa interface.

10. The WLAN AN forwards the EAP-Request/AKA'-Challenge message to the UE.

11. At receipt of the RAND and AUTN in the EAP-Request/AKA'-Challenge message, the ME shall obtain the Access Network Identity from the EAP signalling and the USIM in the UE shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [40]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK' using the Access Network Identity as the KDF input parameter. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3.3. The UE may derive MSK from CK’ and IK’ as per Annex F and as described in RFC 5448[12]. When the UE is performing NSWO authentication, the KAUSF shall not be generated by the UE.

12. The UE shall send the EAP-Response/AKA'-Challenge message to the WLAN AN.

13. The WLAN AN forwards the EAP-Response/AKA'-Challenge message over the SWa interface to the NSWOF.

14. The NSWOF shall send the Nausf\_UEAuthentication\_Authenticate Request with EAP-Response/AKA'-Challenge message to AUSF.

15. The AUSF shall verify if the received response RES matches the stored and expected response XRES. If the AUSF has successfully verified, it continues as follows to step 16, otherwise it returns an error to the NSWOF. The AUSF shall derive the required MSK key from CK’ and IK’ as per Annex F and as described in RFC 5448[12], based on the NSWO indicator received in step 5. The AUSF shall not generate the KAUSF.

16. The AUSF shall send Nausf\_UEAuthentication\_Authenticate Response message with EAP-Success and MSK key to NSWOF. The AUSF may optionally provide the SUPI to NSWOF. The AUSF/UDM shall not perform the linking increased home control to subsequent procedures (as stated in present document clause 6.1.4).

17. The NSWOF shall send the EAP-success and MSK to WLAN AN over the SWa interface. The EAP-Success message is forwarded from WLAN AN to the UE.

18. Upon receiving the EAP-Success message, the UE derives the MSK as specified in step 11, if it has not derived the MSK earlier. The UE uses MSK as a PMK to perform 4-way handshake to establish a secure connection with the WLAN AN.

# S.4 Roaming

The HPLMN may have a roaming agreement with a VPLMN for NSWO roaming. A roaming UE configured by the HPLMN to use 5G NSWO may try to register onto a WLAN AN that may advertise the HPLMN or a VPLMN (with which the HPLMN has a roaming agreement for NSWO roaming). The roaming architecture options are described in clause 4.2.15 in TS 23.501 [2].

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