**3GPP TSG-CT WG3 Meeting #112eC3-205abc**

**E-Meeting, 04th – 13th November 2020 (Revision of C3-205310)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.561** | **CR** | **0072** | **rev** | **1** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | Correction on PAP/CHAP supporting Rel-15 N1 mode UE | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Qualcomm, Vodafone | | | | | | | | | |
| ***Source to TSG:*** | CT3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-CT, TEI16 | | | | |  | ***Date:*** | | | 2020-10-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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:*** | | For PAP/CHAP point to point authentication protocols in ePCO, the SMF in release 15 and 16 doesn’t support using RADIUS/Diameter protocol for the corresponding PAP/CHAP information elements directly for interaction with external DN-AAA server. To this end, in Reply LS "PAP/CHAP and other point-to-point protocols usage in 5GS" (S2-2004481/C3-203599), SA2 has asked CT3 to consider the necessary enhancement so that usage by R15 UEs is permitted.  TS 24.008 Rel-15 CR 3228 in subclause 10.5.6.3.1 defined "If PAP/CHAP protocol is supported by the UE in N1 mode, the UE can use the PAP/CHAP protocol identifiers in the extended protocol configuration options information element in N1 mode.", Then SMF function in a combined PGW-C/SMF and standalone SMF supporting PAP/CHAP in ePCO for Rel-15 UE is needed. And warning shall be added for PAP/CHAP based on S3-202190 LS reply.  CT1#126e approved LS reply to CT3 C3-205085, also answered "for a given DNN, it is the SMF which determines whether PAP/CHAP or EAP based secondary authentication/authorization is to be used." | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Notes added to Table 8.2.2.2-1 and Table 8.2.2.3-1, to provide the missing SMF support of PAP/CHAP in ePCO for N1 mode UE, in addition it is, also added a warning indicating the external network operator to perform the risk assessment if PAP/CHAP is used for authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Rel-15 UEs cannot use PAP/CHAP in ePCO in 5GS, and the legacy DN-AAA server not supporting EAP, can not working with 5GS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.2.2.2, 8.2.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st Change \*\*\*

#### 8.2.2.2 IPv4 Non-transparent access to DN

In this case:

- a static or a dynamic IPv4 address belonging to the Intranet/ISP addressing space is allocated to a UE at PDU session establishment. The methods of allocating IP address to the UE are specified in 3GPP TS 23.501 [2]. The allocated IPv4 address is used for packet forwarding within the UPF and for packet forwarding on the Intranet/ISP;

- as a part of the PDU session establishment, the SMF may request user authentication from an external DN-AAA server (i.e. RADIUS, Diameter) belonging to the Intranet/ISP;

- the IPv4 address allocation to the UE may be performed based on the subscription or a local address pool, which belongs to the Intranet/ISP addressing space, provisioned in the SMF; or via the address allocation servers (i.e. DHCPv4, RADIUS DN-AAA, Diameter DN-AAA) belonging to the Intranet/ISP;

- if requested by the UE at PDU session establishment, the SMF may retrieve the Protocol Configuration Options or IPv4 configuration parameters from a locally provisioned database in SMF and/or from some external server (i.e. DHCPv4, RADIUS DN-AAA, Diameter DN-AAA) belonging to the Intranet/ISP;

- the communication between the 5GS and the Intranet/ISP may be performed over any network, even an insecure network, e.g. the Internet. In case of an insecure connection between the UPF and the Intranet/ISP, there may be a specific security protocol in between. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

Table 8.2.2.2-1 summarizes the IPv4 address allocation and parameter configuration use cases between the UE and the SMF that may lead the SMF to interwork with the external DHCPv4, DN-AAA servers. For detailed description of the signalling flows between the UE and the SMF, see the references in the table.

Table 8.2.2.2-1: IPv4 address allocation and parameter configuration use cases

| Signalling use cases between UE and SMF | Signalling use cases between SMF and external servers | | |
| --- | --- | --- | --- |
| Authentication via RADIUS or Diameter DN-AAA server (clauses 11 or 12)  (NOTE 1 NOTE 2 and NOTE x) | IPv4 Address allocation via DHCPv4 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12)  (NOTE 1 and NOTE 2) | IPv4 parameter configuration via DHCPv4 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12)  (NOTE 1 and NOTE 2) |
| (1) IPv4 address allocation and parameter configuration via activation of QoS flow associated with the default QoS rule  (2) IPv4 address allocation and parameter configuration via DHCPv4 signalling from UE towards SMF (NOTE 3) | X | X | X |
| (3) IPv4 address allocation and parameter configuration in untrusted non-3GPP IP access | X | X | X |
| NOTE  1: When the SMF interworks with AAA servers, the DNN may be configured to interwork with either Diameter DN-AAA or RADIUS DN-AAA server.  NOTE  2: If RADIUS DN-AAA or Diameter DN-AAA server is used, the authentication, IPv4 address allocation and parameter configuration signalling may be combined. Similarly, if DHCPv4 server is used for IPv4 address allocation and parameter configuration, the signalling towards the DHCPv4 server may be combined.  NOTE  3: If the authentication and authorization procedure towards RADIUS DN-AAA or Diameter DN-AAA is required, it is performed by the SMF before the DHCPv4 signalling when it receives the initial access request (i.e. Nsmf\_PDUSession\_CreateSMContext).  NOTE x: The N1 mode UE can provide PAP/CHAP user credentials in the ePCO IE when accessing to 5GS on 3GPP and non-3GPP IP accesses. If such information is provided to the SMF, the SMF can perform user authentication with the DN-AAA server based on these credentials, How to perform authentication by the SMF and the DN-AAA server is not specified in this release. | | | |

NOTE: External network operators intending to use PAP/CHAP without proper underlying protection for authentication are warned about the respective vulnerabilities of PAP and CHAP protocols from a security point of view. It’s up to the external network operator to perform the risk assessment if PAP/CHAP is used for authentication.

\*\*\* 2nd Change \*\*\*

#### 8.2.2.3 IPv6 Non-transparent access to DN

When using IPv6 Address Autoconfiguration, the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDU session establishment for 5GS 3GPP or non-3GPP based access, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be stateless. The stateless procedure, which involves only the UE and the SMF, is described in subclause 10.2. 3.

For DNNs that are configured for IPv6 address allocation, the SMF shall only use the Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see IETF RFC 4291 [32].

The SMF indicates to the UE that Stateless Autoconfiguration shall be performed by sending Router Advertisements as described in subclause 10.2.3 and according to the principles defined in IETF RFC 4861 [33] and IETF RFC 4862 [34].

For UE supporting IPv6, IPv6 Stateless Address Autoconfiguration is mandatory.

In this case, the SMF provides the UE with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address is given using stateless address autoconfiguration. This IPv6 address is used for packet forwarding within the UPF and for packet forwarding on the Intranet/ISP.

When an SMF receives an initial access request (i.e. Nsmf\_PDUSession\_CreateSMContext) message, the SMF deduces from local configuration data associated with the DNN:

- The source of IPv6 Prefixes (SMF internal prefix pool, or external address allocation server);

- Any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [13]);

- The protocol, i.e. RADIUS, Diameter or DHCPv6, to be used with the server(s);

- The communication and security feature needed to communicate with the server(s).

As an example, the SMF may use one of the following options:

- SMF internal Prefix pool for IPv6 prefixes allocation and no authentication;

- SMF internal Prefix pool for IPv6 prefixes allocation and RADIUS for authentication. The RADIUS DN-AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the SMF;

- RADIUS for authentication and IPv6 prefix allocation. The RADIUS DN-AAA server responds with either an Access‑Accept or an Access-Reject to the RADIUS client in the SMF.

The SMF includes the IPv6 address composed of a Prefix and an Interface-Identifier in the initial access response (Namf\_Communication\_N1N2MessageTransfer). The Interface-Identifier may have any value and it does not need to be unique within or across DNNs. It shall however not conflict with the Interface-Identifier that the SMF has selected for its own side of the UE-SMF link. The Prefix assigned by the SMF or the external DN-AAA server shall be globally or site-local unique (see the Note in subclause 11.3 of this document regarding the usage of site-local addresses).

Table 8.2.2.3-1 summarizes the IPv6 prefix allocation and parameter configuration use cases between the UE and the SMF that may lead the SMF to interwork with the external RADIUS DN-AAA, Diameter DN-AAA and DHCPv6 servers. For detailed description of the signalling flows between the UE and the SMF, see the references in the table.

Table 8.2.2.3-1: IPv6 prefix allocation and parameter configuration use cases

| Signalling use cases between UE and SMF | Signalling use cases between SMF and external servers | | |
| --- | --- | --- | --- |
| Authentication via RADIUS or Diameter DN-AAA server (clauses 11 or 12)  (NOTE 1 NOTE 2 and NOTE y) | IPv6 prefix allocation via DHCPv6 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12)  (NOTE 1 and NOTE 2) | IPv6 parameter configuration via DHCPv6 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12)  (NOTE 1 and NOTE 2) |
| (1) IPv6 address allocation and parameter configuration  (2) IPv6 parameter configuration via stateless DHCPv6 | X | X | X |
| (3) IPv6 address allocation and parameter configuration in untrusted non-3GPP IP access | X | X | X |
| NOTE  1: When the SMF interworks with DN-AAA servers, the DNN may be configured to interwork with either Diameter DN-AAA or RADIUS DN-AAA server.  NOTE  2: If RADIUS DN-AAA or Diameter DN-AAA server is used, the authentication, IPv6 prefix allocation and parameter configuration signalling may be combined. Similarly, if DHCPv6 server is used for IPv6 prefix allocation and parameter configuration, the signalling towards the DHCPv6 server may be combined.  NOTE y: The N1 mode UE can provide PAP/CHAP user credentials in the ePCO IE when accessing to 5GS on 3GPP and non-3GPP IP accesses. If such information is provided to the SMF, the SMF can perform user authentication with the DN-AAA server based on these credentials, How to perform authentication by the SMF and the DN-AAA server is not specified in this release. | | | |

NOTE: External network operators intending to use PAP/CHAP without proper underlying protection for authentication are warned about the respective vulnerabilities of PAP and CHAP protocols from a security point of view. It’s up to the external network operator to perform the risk assessment if PAP/CHAP is used for authentication.

For IPv6 the PDU session establishment phase is followed by an address autoconfiguration phase. IPv6 prefix is delivered to UE in Router Advertisement message from the SMF which acts as an access router, in the process of IPv6 Stateless Address Autoconfiguration as described in subclause 10.2.2. Besides DHCPv6 protocol, the SMF may also use RADIUS or Diameter protocol for the retrieval of an IPv6 prefix from external DN.

\*\*\* End of Changes \*\*\*