**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220392-r1***

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1332** | **rev** | **-1** | **Current version:** | **15.14.1** |  |
|  | | | | | | | | |
| *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:*** | on separate handling of N32-c and N32-f | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI15 | | | | |  | ***Date:*** | | | 2022-02-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-15 |
|  | *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:*** | | In the LS S3-201464, SA3 agreed to align TS 33.501 with TS 29.573 and make N32-c connections short-lived. This alignment was done in the CR S3-202208. However, the alignment is not complete and there are still formulations in TS 33.501 that assume N32-c to be long-lived. This is in conflict e.g. with clause 4.3.2.4 of TS 29.573 which states "Once the initial handshake is completed the connection is torn down as specified in 3GPP TS 33.501".  Furthermore, the definition of N32-c connection misses that N32-c is also used for the negotiation of the protection mechanism for the N32-f interface.  Separate TLS connections are setup for N32-c and for N32-f, as per clause 4.3.2.4 of 29.573. Different services are supported for N32-c and N32-f and standards should not preclude SEPP implementation exposing different endpoints for these services. Last but not least separate TLS connections for different services are in line with separation of duties as security principle.  Further, Stage 2 specification provides an ambiguity with respect to this common agreement.  Clause 13.2.2.2 is solely on PRINS, so the last bullet does not belong there.  Similarly, clause 13.5 is contradicting 29.273. See 4.2.3, which says:  If TLS is the negotiated security policy between the SEPP, then the N32-f shall involve only the forwarding of the HTTP/2 messages of the NF service producers and the NF service consumers without any reformatting.  Therefore, it is proposed to align this and provide an explanation in the intro section. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update of the respective clause and clearly stating that different TLS connections are used for N32-c and N32-f.  Changes N32-c to be short-lived instead of long-lived, in the remaining occasions.  Clarifies in the definition of N32-c connection that N32-c is also used for the negotiation of the protection mechanism of the N32-f interface.  Shift and correct text from the PRINS-only clause 13.2.2.2 to clause 13.1.2  Align clause 13.5 with 29.273 clause 4.2.3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Ambiguity and non-alignment between stage 2 and stage 3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.1, 13.1.2, 13.2.2.2, 13.5 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3-220392 | | | | | | | | |

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

## 3.1 Definitions

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

**5G security context:** The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.

NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.

NOTE 2: A 5G security context has type "mapped", "full native" or "partial native". Its state can either be "current" or "non-current". A context can be of one type only and be in one state at a time. The state of a particular context type can change over time. A partial native context can be transformed into a full native. No other type transformations are possible.

**5G AS security context for 3GPP access:** The cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UE security capabilities, and the UP Security Policy at the network side, UP security activation status and the counters used for replay protection.

NOTE 3: NH and NCC need to be stored also at the AMF during connected mode.

NOTE 4: UP security activation status is sent from gNB/ng-eNB in step 1b in clause 6.6.2 corresponding to the active PDU session(s).

**5G AS security context for non-3GPP access:** The key KN3IWF, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec SA.

**5G AS Secondary Cell security context**: The cryptographic keys at AS level for secondary cell with their identifiers, the identifier of the selected AS level cryptographic algorithms for secondary cell, the UP Security Policy at the network side, and counters used for replay protection.

**5G** **Home Environment Authentication Vector:** authentication data consisting of RAND, AUTN, XRES\*, and KAUSF for the purpose of authenticating the UE using 5G AKA.

NOTE 3a: This vector is received by the AUSF from the UDM/ARPF in the Nudm\_Authentication\_Get Response.

**5G Authentication Vector:** authentication data consisting of RAND, AUTN, HXRES\*, and KSEAF.

NOTE 3b: This vector is received by the SEAF from the AUSF in the Nausf\_Authentication\_Authenticate Response.

**5G NAS security context:** The key KAMF with the associated key set identifier, the UE security capabilities, the uplink and downlink NAS COUNT values.

NOTE 4: The distinction between native 5G security context and mapped 5G security context also applies to 5G NAS security contexts. The 5G NAS security context is called "full" if it additionally contains the integrity and encryption keys and the associated identifiers of the selected NAS integrity and encryption algorithms.

**5G Serving Environment Authentication Vector:** a vector consisting of RAND, AUTN and HXRES\*.

**ABBA parameter:** Parameter that provides antibidding down protection of security features against security features introduced in higher release to a lower release and indicates the security features that are enabled in the current network.

**activation of security context:** The process of taking a security context into use.

**anchor key:** The security key KSEAF provided during authentication and used for derivation of subsequent security keys.

**application Layer Security:** mechanism by which HTTP messages, exchanged between a Network Function in one PLMN and a Network Function in another PLMN, are protected on the N32-f interface between the two SEPPs in the two PLMNs.

**authentication data:** An authentication vectoror transformed authentication vector.

**authentication vector:** A vector consisting of CK, IK, RAND, AUTN, and XRES.

**backward security**: The property that for an entity with knowledge of Kn, it is computationally infeasible to compute any previous Kn-m (m>0) from which Kn is derived.

NOTE 5: In the context of KgNB key derivation, backward security refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to compute any previous KgNB that has been used between the same UE and a previous gNB.

**CM-CONNECTED state:** This is as defined in TS 23.501 [2].

NOTE5a: The term CM-CONNECTED state corresponds to the term 5GMM-CONNECTED mode used in TS 24.501 [35].

**CM-IDLE state:** As defined in TS 23.501 [2].

NOTE5b: The term CM-IDLE state corresponds to the term 5GMM-IDLE mode used in TS 24.501 [35].

**consumer's IPX (cIPX):** IPX provider entity with a business relationship with the cSEPP operator.

**consumer's SEPP (cSEPP):** The SEPP residing in the PLMN where the service consumer NF is located.

**current 5G security context:** The security context which has been activated most recently.

NOTE5c: A current 5G security context originating from either a mapped or native 5G security context can exist simultaneously with a native non-current 5G security context.

**forward security**: The fulfilment of the property that for an entity with knowledge of Km that is used between that entity and a second entity, it is computationally infeasible to predict any future Km+n (n>0) used between a third entity and the second entity.

NOTE 6: In the context of KgNB key derivation, forward security refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to predict any future KgNB that will be used between the same UE and another gNB. More specifically, n hop forward security refers to the property that a gNB is unable to compute keys that will be used between a UE and another gNB to which the UE is connected after n or more handovers (n=1 or more).

**full native 5G security context:** A native 5G security context for which the 5G NAS security context is full according to the above definition.

NOTE6a: A full native 5G security context is either in state "current" or state "non-current".

**Home Network Identifier:** An identifier identifying the home network of the subscriber.

NOTE6b: Described in detail in TS 23.003 [19].

**Home Network Public Key Identifier:** An identifier used to indicate which public/private key pair is used for SUPI protection and de-concealment of the SUCI.

NOTE6c: Described in this document and detailed in TS 23.003 [19].

**IAB-donor-CU**: As defined in TS 38.401 [78] .

**IAB-donor-DU**: As defined in TS 38.401 [78].

**IAB-node**: As defined in TS 38.300 [52].

**IAB-donor gNB**:As defined in TS 38.300 [52].

**IAB-UE**: The function within an IAB node, which behaves as a UE.

**mapped 5G security context**: An 5G security context, whose KAMF was derived from EPS keys during interworking and which is identified by mapped ngKSI.

**Master node**: As defined in TS 37.340 [51].

**N32-c connection:** A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN.

NOTE 6d: This is a short-lived connection that is used between the SEPPs for negotiation of the N32-f protection mechanism, cipher suite and protection policy exchange, and error notifications.

**N32-f connection:** Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages.

NOTE 6e: When IPX providers are present in the path between the two SEPPs, an N32-f HTTP connection is setup on each hop towards the other SEPP.

**native 5G security context:** An 5G security context, whose KAMF was created by a run of primary authentication and which is identified by native ngKSI.

**ng-eNB**: As defined in TS 38.300 [52].

**NG-RAN node**: gNB or ng-eNB (as defined in TS 38.300 [52]).

**non-current 5G security context:** A native 5G security context that is not the current one.

NOTE 7: A non-current 5G security context may be stored along with a current 5G security context in the UE and the AMF. A non-current 5G security context does not contain 5G AS security context. A non-current 5G security context is either of type "full native" or of type "partial native".

**partial native 5G security context:** A partial native 5G security context consists of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values, which are initially set to zero before the first NAS SMC procedure for this security context.

NOTE 8: A partial native 5G security context is created by primary authentication, for which no corresponding successful NAS SMC has been run. A partial native context is always in state "non-current".

**producer's IPX (pIPX)**: IPX provider entity with a business relationship with the pSEPP operator.

**producer's SEPP (pSEPP):** The SEPP residing in the PLMN where the service producer NF is located.

**Protection Scheme Identifier:** An identifier identifying a protection scheme that is used for concealing the SUPI.

**RM-DEREGISTERED state:** This is as defined in TS 23.501 [2].

NOTE8a: The term RM-DEREGISTERED state corresponds to the term 5GMM-DEREGISTERED mode used in TS 24.501 [35].

**RM-REGISTERED state:** As defined in TS 23.501 [2].

NOTE8b: The term RM-REGISTERED state corresponds to the term 5GMM-REGISTERED mode used in TS 24.501 [35].

**Routing Indicator:** An indicator defined in TS 23.003 [19] that can be used for AUSF or UDM selection.

**Scheme Output**: the output of a public key protection scheme used for SUPI protection.

**security anchor function:** The function SEAF that serves in the serving network as the anchor for security in 5G.

**Secondary node**: As defined in TS 37.340 [51].

**subscription credential(s):** The set of values in the USIM and in the home operator's network, consisting of at least the long-term key(s) and the subscription identifier SUPI, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.

**subscription identifier:** The SUbscription Permanent Identifier (SUPI).

NOTE8c: As defined in TS 23.501 [2] and detailed in 23.003 [19].

**subscription concealed identifier:** A one-time use subscription identifier, called the SUbscription Concealed Identifier (SUCI), which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.

NOTE8d: Defined in the present document; detailed in TS 23.003 [19].

**subscription identifier de-concealing function:** The Subscription Identifier De-concealing Function (SIDF) service offered by the network function UDM in the home network of the subscriber responsible for de-concealing the SUPI from the SUCI.

**transformed authentication vector:** an authentication vector where CK and IK have been replaced with CK' and IK'.

**UE 5G security capability:** The UE security capabilities for 5G AS and 5G NAS.

**UE security capabilities:** The set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE.

NOTE 9: This includes capabilities for NG-RAN and 5G NAS, and includes capabilities for EPS, UTRAN and GERAN if these access types are supported by the UE.

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

### 13.1.2 Protection between SEPPs

TLS shall be used for N32-c connections between the SEPPs.

If there are no IPX providers between the SEPPs, TLS shall be used for N32-f connections between the SEPPs. Different TLS connections are used for N32-c and N32-f. If there are IPX providers which only offer IP routing service between SEPPs, either TLS or PRINS (application layer security) shall be used for protection of N32-f connections between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

If there are IPX providers which, in addition to IP routing, offer other services that require modification or observation of the information and/or additions to the information sent between the SEPPs, PRINS shall be used for protection of N32-f connections between the SEPPs.

NOTE 1a: The procedure specified in clause 13.5 for security mechanism selection between SEPPs allows SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32, and provides robustness and future-proofness, e.g. in case new algorithms are introduced in the future.

If PRINS is used on the N32-f interface, one of the following additional transport protection methods should be applied between SEPP and IPX provider for confidentiality and integrity protection:

- NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5], or

- TLS VPN with mutual authention following the profile given in clause 6.2 of TS 33.210 [3] and clause clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks, with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

NOTE 1: Void

NOTE 2: Void.

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

13.2.2.2 Procedure for Key agreement and Parameter exchange

1. The two SEPPs shall perform the following cipher suite negotiation to agree on a cipher suite to use for protecting NF service related signalling over N32-f.

1a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP’s supported cipher suites. The cipher suites shall be ordered in initiating SEPP’s priority order. The SEPP shall provide an initiating SEPP’s N32-f context ID for the responding SEPP.

1b. The responding SEPP shall compare the received cipher suites to its own supported cipher suites and shall select, based on its local policy, a cipher suite, which is supported by both initiating SEPP and responding SEPP.

1c. The responding SEPP shall send a Security Parameter Exchange Response message to the initiating SEPP including the selected cipher suite for protecting the NF service related signalling over N32. The responding SEPP shall provide a responding SEPP’s N32-f context ID for the initiating SEPP.

2. The two SEPPs may perform the following exchange of Data-type encryption policies and Modification policies. Both SEPPs shall store protection policies sent by the peer SEPP:

2a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP’s Data-type encryption policies, as described in clause 13.2.3.2, and Modification policies, as described in clause 13.2.3.4.

2b. The responding SEPP shall store the policies if sent by the initiating SEPP.

2c. The responding SEPP shall send a Security Parameter Negotiation Response message to the initiating SEPP with the responding SEPP’s suite of protection policies.

2d. The initiating SEPP shall store the protection policy information if sent by the responding SEPP.

3. The two SEPPs shall exchange IPX security information lists that contain information on IPX public keys or certificates that are needed to verify IPX modifications at the receiving SEPP.

4. The two SEPPs shall export keying material from the TLS session established between them using the TLS export function. For TLS 1.2, the exporter specified in RFC 5705 [61] shall be used. For TLS 1.3, the exporter described in section 7.5 of RFC 8446 [60] shall be used. The exported key shall be used as the master key to derive session keys and IVs for the N32-f context as specified in clause 13.2.4.4.1.

5. The responding SEPP in the first N32-c connection shall now setup a second N32-c connection by establishing a mutually authenticated TLS connection with the peer SEPP.

6. The two SEPPs start exchanging NF to NF service-related signalling over N32-f and tear down the N32-c connection. The SEPPs may initiate new N32-c TLS sessions for any further N32-c communication that may occur over time while application layer security is applied to N32-f.

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

## 13.5 Security capability negotiation between SEPPs

The security capability negotiation over N32-c allows the SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32-f. There shall be an agreed security mechanism between a pair of SEPPs before conveying NF service-related signalling over N32-f.

When a SEPP notices that it does not have an agreed security mechanism for N32-f protection with a peer SEPP or if the security capabilities of the SEPP have been updated, the SEPP shall perform security capability negotiation with the peer SEPP over N32-c in order to determine, which security mechanism to use for protecting NF service-related signalling over N32-f. Certificate based authentication shall follow the profiles given in 3GPP TS 33.210 [3], clause 6.2.

When a SEPP are preconfigured with an agreed security mechanism for N32-f protection with a peer SEPP and the agreed security mechanism is TLS, the SEPPs shall directly forward the NF service related signalling over N32-f using a TLS connection.

A mutually authenticated TLS connection as defined in clause 13.1 shall be used for protecting security capability negotiation over N32-c. The TLS connection shall provide integrity, confidentiality and replay protection.



Figure 13.5-1 Security capability negotiation

1. The SEPP which initiated the TLS connection shall issue a POST request to the exchange-capability resource of the responding SEPP including the initiating SEPP’s supported security mechanisms for protecting the NF service-related signalling over N32-f (see table Table 13.5-1). The security mechanisms shall be ordered in the initiating SEPP’s priority order.

2. The responding SEPP shall compare the received security capabilities to its own supported security capabilities and selects, based on its local policy (e.g. based on whether there are IPX providers on the path between the SEPPs), a security mechanism, which is supported by both initiating SEPP and responding SEPP.

3. The responding SEPP shall respond to the initiating SEPP with the selected security mechanism for protecting the NF service-related signalling over N32.

Table 13.5-1: NF service-related signalling traffic protection mechanisms over N32

|  |  |
| --- | --- |
| N32-f protection mechanism | Description |
| Mechanism 1 | PRINS (described in clause 13.2) |
| Mechanism 2 | TLS |
| Mechanism n | Reserved |

If the selected security mechanism is PRINS, the SEPPs shall behave as specified in clause 13.2.

If the selected security mechanism is TLS, the SEPPs shall behave as specified in clause 13.1.2, tear down the N32-c connection and forward the NF service related signalling over N32-f using a TLS connection.

If the selected security mechanism is a mechanism other than the ones specified in Table 13.5-1, the two SEPPs shall terminate the N32-c TLS connection.

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