**3GPP TSG-SA3 Meeting #100e *S3-201841-r3***

**e-meeting, 17 -24 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0914** | **rev** |  | **Current version:** | **15.9.0** |  |
|  | | | | | | | | |
| *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:*** | Change the long-lived TLS connection of N32-C to the short-lived | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicion, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 21/07/2020 |
|  |  | | | |  | |  | | |  |
| ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | CT4 defined that the N32-C is a short-lived TLS connection. However, SA3 defined that the N32-C is a long-lived TLS connection. During the SA3 #99e meeting, it was agreed to align with CT4. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify that the N32-C is a short-lived TLS connection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misallignment between SA3 and CT4 specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.1, 13.2.2.2, 13.2.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the 1st change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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.

**applicaton 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’s used between the SEPPs for 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of the 1st change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the 2nd 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 a N32-f precontext ID for the responding SEPP. The precontext IDs are 32-bit random integers, represented as 0-left padded strings of hexadecimal digits.

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 N32-f precontext ID for the initiating SEPP.

1d. The SEPPs shall create the N32-f context ID as follows:

Initiating SEPP’s N32-f precontext ID | responding SEPP’s N32-f precontext ID

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-fand may keep the TLS session open for:

- any further N32-c communication that may occur over time while application layer security is applied to N32-f, or

- any further N32-c and N32-f communication, if TLS is used to protect N32-f.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of the 2nd change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of the 3rd change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 13.2.2.3 Procedure for error detection and handling in SEPP

Errors can occur on an active N32-c connection or on one or more N32-f connections between two SEPPs.

When an error is detected, the SEPP shall map the error to an appropriate cause code. The SEPP shall create a signalling message to inform the peer SEPP, with cause code as one of its parameters.

The SEPP shall use the N32-c connection to send the signalling message to the peer SEPP. If the old N32-c connection has been terminated, it uses a new N32-c connection instead.

If the error occurred in the processing of the one or more N32-f message(s), the SEPP shall include the corresponding message ID (s), obtained from the metadata section of the N32-f message, as a parameter in the signalling message. This allows the peer SEPP to identify the source message(s) (HTTP Request or Response) on which the other SEPP found the error.

NOTE: Local action taken by either SEPP is out of 3GPP scope.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of the 3rd change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*