**3GPP TSG-SA3 Meeting #106-e *S3-22xxxx***

e-meeting, 14 - 25 February 2022 (revision of S3-yyxxxx)

**Source: Nokia, Nokia Shanghai Bell**

**Title: New SID on** **Secure RRC Connection setup**

**Document for: Approval**

**Agenda Item:**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

# Title: Study on 5G Secure RRC Connection setup

## Acronym: FS\_RRCCon\_Setup

## Unique identifier: *TBA*

## Potential target Release: Rel-18

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X | X | X |  |
| No |  |  |  |  |  |
| Don't know | X |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | Work Task |
| X | Study Item |

## 2.2 Parent Work Item

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text} |

Dependency on non-3GPP (draft) specification: N/A

# 3 Justification

Existing 3GPP RRC Connection setup (RRC Msg5) is not secure. This lack of security causes issues in multiples features and instances.

-Since security is lacking for RRC Msg5, the UE cannot share any sensitive information with the AMF/network or the base station.

-This is a basic issue for multiple features, for e.g. in Network Slicing, Non terrestrial networks etc.

If this Msg5 is made secure,

-Network Slice selection parameter could be included outside the NAS packet for BS to parse and route the NAS RR to correct AMF in the desired NS.

-For Non-Terrestrial UEs, location information can be included outside the NAS packet for BS to parse and route the NAS RR to correct AMF.

-Msg5 is the last of the remaining messages to be secured and if this is secured a host of issues can be solved with multiple features, like Network Slicing, NTN etc.

Considering the above lack of security for RRC Msg5, there is a need to consider a security study in SA WG3 to make this message secure before the primary authentication of the UE and UE specific NAS and AS contexts are setup.

# 4 Objective

The objectives of this study are to:

1. Study security mechanisms to secure the RRC connection setup procedure so that sensitive information can be shared between genuine network elements BS and AMF even before UE is authenticated and UE specific security context is established.
   1. Secure RRC connection setup should be possible for both roaming and non-roaming UEs, and solutions for both type of UEs are under the scope of the study.
   2. Once the UE is authenticated and UE specific NAS and AS security contexts are established, as currently done, messages shall be protected by the UE specific security context.
   3. Parameters within the RRC connection setup messages are not within the scope of the study. They will be defined by respective WGs as necessary based on features.
2. Conclude on selected solutions for potential normative work.

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | 33.xxx | Study on 5G Secure RRC Connection setup | TSG#98 | TSG#99 | Rakshesh P Bhatt, Nokia, rakshesh.p\_bhatt@nokia.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
| N/A | N/A | N/A | N/A |

# 6 Work item Rapporteur(s)

Rakshesh P Bhatt, Nokia, rakshesh.p\_bhatt@nokia.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Potential interactions with SA2 for the architectural aspects, and RAN 2/3 for the RAN architectural aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Nokia |
| Nokia Shanghai Bell |
|  |
|  |
|  |
|  |
|  |