**Third Generation Partnership Project (3GPP™)**

 **Meeting Report
for
TSG SA WG3
meeting: 94AH**

**Stockholm, Sweden, 11/03/2019 to 15/03/2019**

Contents:

1 Opening of the meeting 3

2 Approval of Agenda and Meeting Objectives 3

3 IPR and Anti-Trust Law Reminder 3

4 Work Areas 4

4.1 Security Assurance Specification for 5G (SCAS\_5G) (Rel-16) 4

4.1.1 NR Node B (gNB) (TS 33.511) 4

4.1.2 Access and Mobility Management Function (TS 33.512) 4

4.1.3 User Plane Function (UPF) (TS 33.513) 4

4.1.4 Unified Data Management (UDM) (TS 33.514) 5

4.1.5 Session Management Function (SMF) (TS 33.515) 5

4.1.6 Authentication Server Function (AUSF) (TS 33.516) 6

4.1.7 Security Edge Protection Proxy (SEPP) (TS 33.517) 6

4.1.8 Network Resource Function (NRF) (TS 33.518) 7

4.1.9 Network Exposure Function (NEF) (TS 33.519) 8

4.1.10 Other issues 8

5 Studies 10

5.1 Study on Security Aspects of the 5G Service Based Architecture (FS\_SBA-Sec) (Rel-16) 10

5.2 Study on Long Term Key Update Procedures (FS\_LTKUP) (Rel-16) 16

5.3 Study on Supporting 256-bit Algorithms for 5G (FS\_256-Algorithms) (Rel-16) 16

5.4 Security aspects of single radio voice continuity from 5G to UTRAN (FS\_5G\_UTRAN\_SEC) (Rel-16) 16

5.5 Study on authentication and key management for applications based on 3GPP credential in 5G IoT (FS\_AKMA) (Rel-16) 16

5.6 Study on evolution of Cellular IoT security for the 5G System (FS\_CIoT\_sec\_5G) (Rel-16) 25

5.7 Study on the security of the Wireless and Wireline Convergence for the 5G system architecture (FS\_5WWC\_SEC) (Rel-16) 29

5.8 Study on Security Aspects of PARLOS (FS\_PARLOS\_Sec) (Rel-16) 33

5.9 Study on 5G security enhancement against false base stations (FS\_5GFBS) (Rel-16) 35

5.10 Study of KDF negotiation for 5G System Security (FS\_5GS\_KDF) (Rel-16) 47

5.11 Study on Security aspects of Enhancement of Network Slicing (FS\_eNS\_SEC) (Rel-16) 47

5.12 Study on Security of the enhancement to the 5GC location services (FS\_eLCS\_Sec) (Rel-16) 52

5.13 Study on security for 5G URLLC (FS\_5G URLLC\_SEC) (Rel-16) 57

5.14 Study on SECAM and SCAS for 3GPP virtualized network products (FS\_VNP\_SECAM\_SCAS) (Rel-16) 63

5.15 Study on Security for 5GS Enhanced support of Vertical and LAN Services (FS\_Vertical\_LAN\_SEC) (Rel-16) 64

5.16 Study on LTKUP Detailed solutions (FS\_LTKUP\_Detail) (Rel-16) 70

5.17 Study on User Plane Integrity Protection (FS\_UP\_IP\_Sec) (Rel-16) 72

5.18 Study on Security Impacts of Virtualisation (FS\_SIV) (Rel-16) 77

5.19 Study on authentication enhancements in 5GS (FS\_AUTH\_ENH) (Rel-16) 78

5.20 Study on Security for NR Integrated Access and Backhaul (FS\_NR\_IAB\_Sec) 84

5.21 Study on Security Aspects of 3GPP support for Advanced V2X Services (FS\_eV2X\_Sec) 85

6 Any Other Business 86

Annex A: List of contribution documents 88

Annex B: Lists of liaisons 101

B1: Incoming liaison statements 101

B2: Outgoing liaison statements 101

Annex C: List of draft Technical Specifications and Reports 102

Annex D: List of participants 103

Annex E: List of future meetings 106

## 1 Opening of the meeting

## 2 Approval of Agenda and Meeting Objectives

**S3-190600 Agenda**

 *Type: agenda For: (not specified)
 Source: WG Vice Chair*

**Discussion:**

Revised to correct editorial and add proposed schedule. Ericsson provided a welcome presentation. Chair reminded everyone of IT being a shared facility. Chair provided IPR policy and a reminder of the anti-trust issues.

**Decision:** The document was **revised to S3-190921**.

**S3-190921 Agenda**

 *Type: agenda For: -
 Source: WG Vice Chair*

(Replaces S3-190600)

**Decision:** The document was **approved**.

## 3 IPR and Anti-Trust Law Reminder

The attention of the delegates to the meeting of this Technical Specification Group was drawn to the fact that 3GPP Individual Members have the obligation under the IPR Policies of their respective Organizational Partners to inform their respective Organizational Partners of Essential IPRs they become aware of.

The delegates were asked to take note that they were thereby invited:

to investigate whether their organization or any other organization owns IPRs which were, or were likely to become Essential in respect of the work of 3GPP.

to notify their respective Organizational Partners of all potential IPRs, e.g., for ETSI, by means of the IPR Information Statement and the Licensing declaration forms.

The attention of the delegates to the meeting was drawn to the fact that 3GPP activities were subject to all applicable antitrust and competition laws and that compliance with said laws was therefore required by any participant of the meeting, including the Chairman and Vice-Chairmen and were invited to seek any clarification needed with their legal counsel. The leadership would conduct the present meeting with impartiality and in the interests of 3GPP.

Delegates were reminded that timely submission of work items in advance of TSG/WG meetings was important to allow for full and fair consideration of such matters. Delegates were reminded of the fair network use rules established by the PCG:

1. Users shall not use the network to engage in illegal activities. This includes activities such as copyright violation, hacking, espionage or any other activity that may be prohibited by local laws.

2. Users shall not engage in non-work related activities that are consume excessive bandwidth or cause significant degradation of the performance of the network.

## 4 Work Areas

### 4.1 Security Assurance Specification for 5G (SCAS\_5G) (Rel-16)

#### 4.1.1 NR Node B (gNB) (TS 33.511)

#### 4.1.2 Access and Mobility Management Function (TS 33.512)

**S3-190740 SCAS: AMF-specific adaptations of security functional requirements and related test cases**

 *Type: pCR For: Approval
 33.512 v0.5.0
 Source: Huawei, Hisilicon*

**Discussion:**

It was questioned whether the test case in 4.2.2.1.X.1 was needed - it was agreed that this was not needed. For 4.2.2.Y.1 test case, an EN "Security objectives and threat need to be added with reference to TS 33.926" was agreed to be added. The expected result of 4.2.2.Y.1 was taken offline. Same EN for 4.2.2.Y.2, 4.2.2.Z.1 and 4.2.2.Z.2 was agreed. Taken offline whether 4.2.2.Y.2 needs to consider handovers. No other changes for 4.2.2.Z.1. 4.2.2.Z.2 taken offline to see if it can be merged with 4.2.2.Z.1.

**Decision:** The document was **revised to S3-190884**.

**S3-190884 SCAS: AMF-specific adaptations of security functional requirements and related test cases**

 *Type: pCR For: Approval
 33.512 v0.5.0
 Source: Huawei, Hisilicon*

(Replaces S3-190740)

**Decision:** The document was **approved**.

**S3-190887 Draft TS 33.512**

 *Type: draft TS For: Approval
 33.512 v0.6.0
 Source: Deutsche Telekom*

**Decision:** The document was **approved**.

#### 4.1.3 User Plane Function (UPF) (TS 33.513)

**S3-190741 Security Assurance Requirements and Test Case for UPF**

 *Type: pCR For: Approval
 33.513 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

It was questioned whether confidentiality and integrity need to be separate test cases - it was agreed to merge them. It was questioned whether the test cases are needed at all as the general test case already exists in TS 33.117. The Pre-Condition should not refer to a PLMN as it is always in a test lab - proposal to remove "if .." and make the test mandatory was agreed. EN "Security objectives and threat need to be added with reference to TS 33.926" was agreed to be added. It was proposed to remove Y2 to Y5 test cases as it was not clear that this directly apply. Discussion taken offline on this. The revision of this document (S3-190885) will only consider X1 and Y1. Revision of Y2 to Y5 will be in S3-190886.

**Decision:** The document was **revised to S3-190885**.

**S3-190885 Security Assurance Requirements and Test Case for UPF**

 *Type: pCR For: Approval
 33.513 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190741)

**Decision:** The document was **approved**.

**S3-190886 security Assurance Requirements and Test Case for UPF- Reference to 33.250**

 *Type: pCR For: Approval
 33.513 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **approved**.

**S3-190888 Draft TS 33.513**

 *Type: draft TS For: Approval
 33.513 v0.3.0
 Source: Samsung*

**Decision:** The document was **approved**.

#### 4.1.4 Unified Data Management (UDM) (TS 33.514)

#### 4.1.5 Session Management Function (SMF) (TS 33.515)

**S3-190743 Security Assurance Requirement and test cases for SMF**

 *Type: pCR For: Approval
 33.515 v0.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

There was no support and several people against including the first test case - this will not be included. Test 2 will be included with "The tester captures the N1 initial context setup message." clarified that this on N2 interface and EN "Security objectives and threat need to be added with reference to TS 33.926". There was no support and several people against including the third and fourth test cases - these will not be included. Change 5 needs to be aligned with the remaining test case.

**Decision:** The document was **revised to S3-190889**.

**S3-190889 Security Assurance Requirement and test cases for SMF**

 *Type: pCR For: Approval
 33.515 v0.1.0
 Source: Huawei, Hisilicon*

(Replaces S3-190743)

**Decision:** The document was **approved**.

**S3-190890 draft TS 33.515**

 *Type: draft TS For: Approval
 33.515 v0.2.0
 Source: Huawei*

**Decision:** The document was **approved**.

#### 4.1.6 Authentication Server Function (AUSF) (TS 33.516)

#### 4.1.7 Security Edge Protection Proxy (SEPP) (TS 33.517)

**S3-190637 New Test Case: Error handling of malformed N32 signalling message sent between peer SEPPs**

 *Type: pCR For: Approval
 33.517 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes to add SEPP security requirement and test case related for discarding the malformed N32 signalling message sent between two peer SEPPs.

**Discussion:**

Not security related but generic - some suggestion. that this should go into TS 33.117. This was taken offline to work on what parts need to go into TS 33.117

**Decision:** The document was **noted**.

**S3-190728 Test Case: Connection-specific scope of IPX-provider cryptographic material**

 *Type: pCR For: Approval
 33.517 v0.2.0
 Source: Deutsche Telekom AG*

**Discussion:**

It was agreed that EN "Security objectives and threat need to be added with reference to TS 33.926" and another EN that the requirements need to be TS 33.501.

**Decision:** The document was **revised to S3-190891**.

**S3-190891 Test Case: Connection-specific scope of IPX-provider cryptographic material**

 *Type: pCR For: Approval
 33.517 v0.2.0
 Source: Deutsche Telekom AG*

(Replaces S3-190728)

**Decision:** The document was **approved**.

**S3-190780 SCAS SEPP: Serving PLMN ID Mismatch**

 *Type: pCR For: Approval
 33.517 v0.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Based on the current version of TS 33.517, this paper proposes the test case for correct handling by SEPP when identifying the mismatch between the PLMN-ID contained in the incoming N32-f message and the PLMN-ID in the related N32-f context.

**Discussion:**

It was felt that the threats were not clearly defined. The discussion of the threat description was taken offline. The needs for 'consumer' and 'producer' in the test was questioned - this will be taken offline. The private key should be the test private key. The second expected result is not in TS 33.501 so cannot be added currently.

**Decision:** The document was **revised to S3-190892**.

**S3-190892 SCAS SEPP: Serving PLMN ID Mismatch**

 *Type: pCR For: Approval
 33.517 v0.2.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190780)

**Decision:** The document was **approved**.

**S3-190893 Draft TS 33.517**

 *Type: draft TS For: Approval
 33.517 v0.3.0
 Source: Nokia*

**Decision:** The document was **approved**.

#### 4.1.8 Network Resource Function (NRF) (TS 33.518)

**S3-190742 Security Assurance Requirement and Test for NRF**

 *Type: pCR For: Approval
 33.518 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

It was questioned whether the first test is needed as it is not a security test. This discussion will be taken offline. The second tests seem to check whether the authorisation feature is implemented (i.e. checking functionality) - does this need to be covered. Something needs to be clarified - this will be taken offline. Similar concerns were raised for test case 3.

**Decision:** The document was **revised to S3-190978**.

**S3-190978 Security Assurance Requirement and Test for NRF**

 *Type: pCR For: Approval
 33.518 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190742)

**Discussion:**

Nokia: why incorrect operation leads to so many threats? E//: not clear what are the threats. Come back with threats for next meeting. Huawei: ok, threat discussion.

**Decision:** The document was **noted**.

**S3-190805 SCAS NRF: Scope Representation for Nnrf\_AccessToken Service**

 *Type: pCR For: Approval
 33.518 v0.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Based on the current version of TS 33.518, this paper proposes two new test cases for scope representation for Nnrf\_AccessToken Service, which are NRF-specific security requirements derived from 29.510.

**Discussion:**

It was also questioned whether this is really just testing functionality and what is the security rationale for the test case. There was no support for inclusion of these cases.

**Decision:** The document was **noted**.

#### 4.1.9 Network Exposure Function (NEF) (TS 33.519)

**S3-190618 SCAS NEF Add test steps for authorization on northbound APIs**

 *Type: pCR For: Approval
 33.519 v0.3.0
 Source: ZTE Corporation*

**Discussion:**

The security rationale of the proposed test case was questioned. If with a faked token, the AMF responds then there is a security problem was the response. This was taken offline to fix the execution steps.

**Decision:** The document was **revised to S3-190894**.

**S3-190894 SCAS NEF Add test steps for authorization on northbound APIs**

 *Type: pCR For: Approval
 33.519 v0.3.0
 Source: ZTE Corporation*

(Replaces S3-190618)

**Decision:** The document was **approved**.

**S3-190895 draft TS 33.519**

 *Type: draft TS For: Approval
 33.519 v0.4.0
 Source: ZTE*

**Decision:** The document was **approved**.

#### 4.1.10 Other issues

**S3-190638 New Test Case: Error handling of malformed JSON object between two network products**

 *Type: pCR For: Approval
 33.517 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes to add a generalized security requirement and test case related for discarding the malformed JSON object sent between two network products.

**Discussion:**

What is meant be malformed as if it general, then there could be a test for malformed JSON objects.

**Decision:** The document was **noted**.

**S3-190672 Living Document: General SBA/SBI aspects in TS 33.117**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This is a living document for capturing general SBA/SBI aspects in TS 33.117 for NF-specific SCAS documents to reference.

**Decision:** The document was **revised to S3-190897**.

**S3-190897 Living Document: General SBA/SBI aspects in TS 33.117**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190672)

**Decision:** The document was **approved**.

**S3-190749 The purpose and scope of SCAS**

 *Type: discussion For: Endorsement
 Source: Ericsson*

**Discussion:**

It was commented that test cases should not define new requirements - modify proposal 2 by adding "and where the requirement is documented in a 3GPP TS or TR" This was agreeable. Proposal 1 require the rapporteur to bring in the relevant text for their TS.

**Decision:** The document was **revised to S3-190883**.

**S3-190883 The purpose and scope of SCAS**

 *Type: discussion For: Endorsement
 Source: Ericsson*

(Replaces S3-190749)

**Decision:** The document was **endorsed**.

**S3-190775 SCAS 5G: mutual authentication between NFs**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This paper proposes a new sub-clause under 4.2.2.1 for one general baseline requirement and its corresponding test case applicable to all NFs utilizing SBI, which is mutual authentication between NFs.

**Discussion:**

The proposed test case adds more requirement to an existing test case, so rather than add a new test case it was agreed to work offline to update an existing test cases. The EN "Security objectives and threat need to be added with reference to TS 33.926" was also needed.

**Decision:** The document was **revised to S3-190896**.

**S3-190896 SCAS 5G: mutual authentication between NFs**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190775)

**Decision:** The document was **approved**.

**S3-190777 SCAS 5G: update to Access Token Verification Failure in non-roaming case**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This paper proposes some updates to one of the test cases, which is authorization failure handling of NF service access within the same PLMN.

**Decision:** The document was **approved**.

**S3-190778 SCAS 5G: update to Access Token Verification Failure in roaming case**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This paper proposes some updates to one of the test cases, which is authorization failure handling of NF service access in roaming scenario.

**Decision:** The document was **approved**.

**S3-190779 SCAS 5G: Search Result Handling for NF Discovery**

 *Type: draftCR For: Approval
 33.117 v16.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This paper proposes a new sub-clause under 4.2.2.1 for search result handling applicable to all NFs for NF discovery. The sub-clause contains two test case:

- one is the correct handling by a NF service consumer when receiving search result validity peri

**Discussion:**

No support for this contribution.

**Decision:** The document was **noted**.

## 5 Studies

### 5.1 Study on Security Aspects of the 5G Service Based Architecture (FS\_SBA-Sec) (Rel-16)

**S3-190744 New Key Issue: Support of a UP gateway function on the N9 interface**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Ericsson*

**Discussion:**

Nokia: move to separate subclause in 5.5 of 501 to have separate requirement for N9, shouldn't' stay in TR. DT: should say inform the SEPP. E//: should be on new interface, whatever it is. NEC: why we need that interface to UPF, or if the box is transparent. add new bullet point solution needs to motivate the need for new interface. Juniper: the ? in the figure refer to control plane interface. E//: could update figure. Nokia: have section for N9 requirements in TR.

**Decision:** The document was **revised to S3-190964**.

**S3-190964 New Key Issue: Support of a UP gateway function on the N9 interface**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Ericsson*

(Replaces S3-190744)

**Discussion:**

add EN: N9 requirements go into a separate clause.

**Decision:** The document was **approved**.

**S3-190737 New KI: flexible protection of data exchange on N9**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Juniper: not invent a new protocol for this. E//: need to clarify flexibility. *BT:* The real reason for this is protecting core network not just protecting the user. E//: Huawei: this is a GSMA requirement NCSC: is SEPP-U something decided. DCM: problem with flexibility, when it is about dynamic flexibility. EN: what does flexibility mean. NCSC: first requirement: the system …

**Decision:** The document was **revised to S3-190965**.

**S3-190965 New KI: flexible protection of data exchange on N9**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Huawei, Hisilicon,Nokia*

(Replaces S3-190737)

**Decision:** The document was **approved**.

**S3-190876 Protection of N9 interface in Inter-PLMN scenario**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Protection of N9 interface in Inter-PLMN scenario

**Discussion:**

Juniper: replace the previous contribution. BT: support this. Huawei: issue with lack of flexibility. E//: change requirement to system shall support. Juniper: say according to 33.210. NCSC: why 5GJA wanted flexibility. DCM: send LS to GSMA. Huawei: LS from GSMA was clear already. DCM: unclear if 33.210 is sufficient Nokia: need clarification. E//: add EN from previous contribution, then the previous contribution is captured as well. Nokia: agree.

**Decision:** The document was **merged**.

**S3-190869 Security aspects of Service Communication Proxy (SCP)**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

SRel-16 5GC supports indirect communication via an SCP. Security aspects of SCP must be studied in detail to ensure that there is no loss in security with the introduction of SCP between two NFs

**Discussion:**

together with 726 , merged into 967 and 968

**Decision:** The document was **revised to S3-190967**.

**S3-190967 Security aspects of Service Communication Proxy (SCP)**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell,Deutsche Telekom*

(Replaces S3-190869)

**Decision:** The document was **approved**.

**S3-190726 Key Issue: Protection of SCP interfaces**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Deutsche Telekom AG*

**Decision:** The document was **merged**.

**S3-190727 Key Issue: Secure message transport via the SCP**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Deutsche Telekom AG*

**Discussion:**

E//: need to merge these. Two issues. Requirements: system shall support. On 727: reference should be checked. not refer to NDS/IP

**Decision:** The document was **revised to S3-190968**.

**S3-190968 Key Issue: Secure message transport via the SCP**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Deutsche Telekom AG*

(Replaces S3-190727)

**Decision:** The document was **approved**.

**S3-190871 NF to NF authentication and authorization in Indirect communication mode**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This key issue addresses how NF to NF authentication and authorization works in Indirect communication mode.

**Discussion:**

E//: could be merged to 727. bullet B may no longer be possible DCM: SCoP defines a trust domain. Keep open

**Decision:** The document was **revised to S3-190981**.

**S3-190981 NF to NF authentication and authorization in Indirect communication mode**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190871)

**Decision:** The document was **approved**.

**S3-190872 Authorization of NF service access in SCP**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

In Rel-16, the SCP is expected to support the functionality of OAuth 2.0 based service access authorization of NF service consumer.

**Discussion:**

DT: auth is in SA3 domain, remove second para. E//: check offline about authorization. Third paragraph depends on second para. Nokia: take this offline

**Decision:** The document was **revised to S3-190980**.

**S3-190980 Authorization of NF service access in SCP**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190872)

**Decision:** The document was **approved**.

**S3-190874 Service access authorization within a NF Set or NF Service Set**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Study the impact of instance Set introduced by SA2, on OAuth 2.0 based Service access authorization.

**Discussion:**

E//: looks like solution. Requirement: the 5G system shall support token based authentication NF sets and NF service sets DCM: ist.io may replace oauth based authentication. Leave req as tbd. Accept with tbd, requirements for next meeting. QC: remove SA2, and reference to CR, should be reference to TS. DCM: EN: change to specification after acceptance of CR. Further formatting comments.

**Decision:** The document was **revised to S3-190982**.

**S3-190982 Service access authorization within a NF Set or NF Service Set**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190874)

**Decision:** The document was **approved**.

**S3-190873 Indirect communication between NFs in roaming scenarios**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This key issue studies the use of SCP on the consumer and/or producer side in roaming scenarios and security aspects when indirect communication is used between two NFs in such scenarios

**Discussion:**

E//: remove "something similar…", as it is solution. DCM: this is architectural requirement. Interoperability with R15.

**Decision:** The document was **revised to S3-190983**.

**S3-190983 Indirect communication between NFs in roaming scenarios**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190873)

**Decision:** The document was **approved**.

**S3-190724 Draft LS on SCP security requirements**

 *Type: LS out For: Approval
 to SA2
 Source: Deutsche Telekom AG*

**Discussion:**

TNO: is the SCP already decided? DCM: SA2 decided

**Decision:** The document was **merged**.

**S3-190725 Key Issue: Handling of invalid IPX patches**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Deutsche Telekom AG*

**Discussion:**

DCM: ed note: whether to really do per error cause and per N32 connection is FFS

**Decision:** The document was **revised to S3-190984**.

**S3-190984 Key Issue: Handling of invalid IPX patches**

 *Type: pCR For: Approval
 33.855 v1.3.0
 Source: Deutsche Telekom AG*

(Replaces S3-190725)

**Decision:** The document was **approved**.

**S3-190879 TLMSP, A Proxy Transport Layer Secure Protocol**

 *Type: other For: Discussion
 Source: NCSC*

**Abstract:**

This document is submitted on behalf of ETSI TC Cyber. It provides information on TLMSP, a proxy transport layer secure protocol. TLMSP has similarities to application layer security for N32 and fulfils similar requirements.

**Discussion:**

comments to be given offline

**Decision:** The document was **noted**.

**S3-190966 LS on Clarification of flexibility of N9 protection**

 *Type: LS out For: Approval
 to GSMA 5GJA
 Source: Deutsche Telekom*

**Discussion:**

ask whether 33.210 flexibility is sufficient. DCM: include that there is cost to flexibility. Nokia: granularity clear enough. Telia: what kind of configuration and what is automatic. NCSC: rephrase q1: .., could GSMA 5GJA report on any planned requirements for flexible requirements.

**Decision:** The document was **revised to S3-191016**.

**S3-191016 LS on Clarification of flexibility of N9 protection**

 *Type: LS out For: Approval
 to GSMA 5GJA
 Source: Deutsche Telekom*

(Replaces S3-190966)

**Decision:** The document was **approved**.

**S3-190961 LS on handling of Indirect communication across NF/NF Services**

 *Type: LS in For: Approval
 Original outgoing LS: -, to -, cc -
 Source: S2-1902905*

**Discussion:**

DCM: SCP bad acronym. May need two SCPs one for consumer and for producer DT: have proposal regarding visibility in architecture

**Decision:** The document was **replied to in S3-190963**.

**S3-190963 Reply LS on handling of Indirect communication across NF/NF Services**

 *Type: LS out For: Approval
 to SA2
 Source: Deutsche Telekom*

**Decision:** The document was **approved**.

**S3-191031 Draft TR 33.855**

 *Type: draft TR For: Approval
 33.855 v1.4.0
 Source: Deutsche Telekom*

**Decision:** The document was **approved**.

### 5.2 Study on Long Term Key Update Procedures (FS\_LTKUP) (Rel-16)

### 5.3 Study on Supporting 256-bit Algorithms for 5G (FS\_256-Algorithms) (Rel-16)

### 5.4 Security aspects of single radio voice continuity from 5G to UTRAN (FS\_5G\_UTRAN\_SEC) (Rel-16)

### 5.5 Study on authentication and key management for applications based on 3GPP credential in 5G IoT (FS\_AKMA) (Rel-16)

**S3-190750 New KI: Interworking between AKMA and GBA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Abstract:**

Re-submission of S3-190326 which was not treated in Kochi.

Investigate if interworking between AKMA and GBA introduces any new security concerns.

**Discussion:**

Vodafone: Can KI cover the case for interworking between GBA and AKMA so do not need two systems. Ericsson: That was intention. Vodafone: proposed scenario for inclusion. Huawei: Agree with VDF point and want backwards compatibility with GBA - a new sentence perhaps. Nokia: Generalise the title would help make it clear what the key issue is addressing. TI: Concerned that is not clear what all the use cases are as SA3 are not doing this based on SA1 requirements. Vodafone: Perhaps additions to clause 4 would help. An EN will be added to capture this need. Interdigital: Is this in scope of study. BT: Need interworking to protect operators investment - good to add a security requirement on this - taken offline. Vodafone: Work is in scope as the evolution of GBA.

**Decision:** The document was **noted**.

**S3-190922 New KI: Interworking between AKMA and GBA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Decision:** The document was **withdrawn**.

**S3-190640 Discussion on use of established keys for AKMA root key**

 *Type: discussion For: Discussion
 33.835 v..
 Source: NEC Europe Ltd*

**Abstract:**

This contribution discusses the issue of out-of-sync keys and propose the solution approach.

**Discussion:**

Vodafone: OK to trust VPLMN not to be malicious in this case. Huawei: Why change the AUSF based on the AKMA study. Vodafone: Moving the storage of K\_AUSF may cause backwards compatibility to existing kit - this should be studied.

**Decision:** The document was **noted**.

**S3-190646 New KI on Synchronization of Keys when using established keys**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new KI.

**Decision:** The document was **approved**.

**S3-190702 Key issue on Key freshness in AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **revised to S3-190924**.

**S3-190924 Key issue on Key freshness in AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Huawei, Hisilicon*

(Replaces S3-190702)

**Decision:** The document was **approved**.

**S3-190824 Updates to KI #14**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

Qualcomm: Why does the UE need to revoke the key? Agreed to not have requirement change. Also change the last EN to make it refer to UE only. BT and Vodafone raised scenarios where the key may not be usable in the UE.

**Decision:** The document was **revised to S3-190925**.

**S3-190925 Updates to KI #14**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

(Replaces S3-190824)

**Decision:** The document was **approved**.

**S3-190613 New Solution: Battery efficient AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: KPN N.V.*

**Abstract:**

This solution proposes procedures, signalling, and a key hierarchy to obtain AKMA functionality for battery constrained UEs.

**Discussion:**

It was proposed that the references to BEST were removed. This was agreed. QC: How are the user identity and enterprise id protected, hoes does this work with EAP method and how is this battery efficient. An editor's note of each of these issues was requested. Vodafone: Concern about any claim about battery efficiency - would rather remove any mention of battery efficiency claims. There was support for this view.

**Decision:** The document was **revised to S3-190926**.

**S3-190926 New Solution: Battery efficient AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: KPN N.V.*

(Replaces S3-190613)

**Decision:** The document was **approved**.

**S3-190632 Solution to KI#9 Key separation for AKMA AFs**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This pCR proposes a solution for Key issue #9 specified in study item on AKMA.

**Discussion:**

BT: Add an EN about further key separation to prevent key leakage causing an issue for other cases.

**Decision:** The document was **revised to S3-190927**.

**S3-190927 Solution to KI#9 Key separation for AKMA AFs**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

(Replaces S3-190632)

**Decision:** The document was **approved**.

**S3-190801 pCR: Reusing KAUSF for AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Qualcomm Incorporated*

(Replaces S3-190385)

**Discussion:**

NEC: Key identifier does not provide proof of possession. An EN will be enhanced to capture this. Some editorial corrections were pointed out. There was some discussion on LI, but no changes were need at this meeting.

**Decision:** The document was **revised to S3-190928**.

**S3-190928 pCR: Reusing KAUSF for AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Qualcomm Incorporated*

(Replaces S3-190801)

**Decision:** The document was **approved**.

**S3-190639 Solution for Established Key Synchronization**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new solution for implicit bootstrapping key synchronization.

**Discussion:**

Vodafone: Change of title to make it Key synchronisation for implicit bootstrapping. Ericsson: Will this work/be needed if this is covered by TS 33.501. NEC: Would not need a new solution if TS 33.501 provides a solution. Qualcomm: Propose an EN on the use of ngKSI for AKMA key identification and use identification rather than synchronisation in title.

**Decision:** The document was **revised to S3-190929**.

**S3-190929 Solution for Established Key Synchronization**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

(Replaces S3-190639)

**Decision:** The document was **approved**.

**S3-190642 Resolving Editor’s Notes in Solution #16**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution resolves an existing EN.

**Decision:** The document was **approved**.

**S3-190641 Discussion on using KSEAF and/or KAUSF for AKMA in view of regulatory compliance**

 *Type: discussion For: Discussion
 33.835 v..
 Source: NEC Europe Ltd*

**Abstract:**

This contribution discusses how and why to use KAUSF and/or KSEAF.

**Discussion:**

Orange: Questioning the conclusion on supplying the key to the serving networks - this is not aligned with BEST. DCM: Concerned that there is a large change of trust model as the home operator should be in control of the authentication

**Decision:** The document was **noted**.

**S3-190644 Updating solution #16 to include home network option**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution updates existing solution #16.

**Discussion:**

DCM: Proposal to add an EN in evaluation to cover concern about providing keys to serving networks. Qualcomm proposed that AKMA authentication based from a key known to the serving network loses home network control. Orange and DCM were supportive of such a sentence. This was taken offline.

**Decision:** The document was **revised to S3-190930**.

**S3-190930 Updating solution #16 to include home network option**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

(Replaces S3-190644)

**Decision:** The document was **approved**.

**S3-190645 Creating a combined solution for usage of KSEAF and KAUSF**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new solution.

**Discussion:**

Kept open based on the discussion of S3-190930 -

**Decision:** The document was **revised to S3-190996**.

**S3-190996 Creating a combined solution for usage of KSEAF and KAUSF**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

(Replaces S3-190645)

**Decision:** The document was **approved**.

**S3-190643 Solution for Roaming Architecture**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new solution.

**Discussion:**

Orange: what is the rationale for this proposal. NEC: Similar to GBA to have a proxy in the serving network. Qualcomm: Agree that motivation for proxy is not clear, i.e. is it a routing issue.

**Decision:** The document was **noted**.

**S3-190688 improvement for AKMA architecture**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

Gemalto: What is the rationale for the proxy

**Decision:** The document was **noted**.

**S3-190703 Solution for Key freshness in AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Huawei, Hisilicon*

**Discussion:**

Orange: This relates to S3-190924 - this was closed for a while until the key issue was approved. Ericsson: EN asking for clarification on application key generation. Orange: Key lifetime check is not optional

**Decision:** The document was **revised to S3-191005**.

**S3-191005 Solution for Key freshness in AKMA**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Huawei, Hisilicon*

(Replaces S3-190703)

**Decision:** The document was **approved**.

**S3-190767 AKMA Architecture and procedures with the anchor function as NEF**

 *Type: pCR For: (not specified)
 33.835 v0.3.0
 Source: China Mobile Com. Corporation*

**Discussion:**

Orange: It is not clear what the solution is proposing. The reasons for co-locating the NEF and AApF are not justified

**Decision:** The document was **noted**.

**S3-190774 Resolving Editor's notes in solution 6**

 *Type: pCR For: (not specified)
 33.835 v0.3.0
 Source: China Mobile Com. Corporation*

**Discussion:**

E//: protocol is run on ME. CMCC: yes. E//: add to evaluation EN: it is FFS how a non 3GPP UE implementing COAP, MQTT, etc. can interface to 3GPP network. Orange: what does E// want to study, non 3GPP UE is out of scope. E//: how is COAP and MQTT used to transport 5G protocols. Nokia: there will be a gateway. Orange: instead put an EN on how the protocol stack works. VF: is the author of the previous contribution happy with this substantial change? remove evaluation. CMCC: remove evaluation. VF: not the right process to change other people's solutions. DCM: contributions can change other people's solutions, but if the group decides to not to accept this, or prefers a new solution, then this will be decided.

**Decision:** The document was **revised to S3-190931**.

**S3-190931 Resolving Editor's notes in solution 6**

 *Type: pCR For: -
 33.835 v0.3.0
 Source: China Mobile Com. Corporation*

(Replaces S3-190774)

**Decision:** The document was **approved**.

**S3-190807 Protocol details for solution 3**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190821 Updates to Solution #14**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

VF: out of scope. Lifetime of keys irrelevant to 3GPP. Mechanism to renegotiate a key is in scope E//: key negotiation by revocation. QC: delete all proposed text in 6.14.2.2, replace by text how revocation in UE is out of scope. E//: previous contribution had ed note UE revocation is FFS. QC: ok leave out all this text for now. 6.14.2.2, 6.14.2.3, 6.14.2.3. Nokia: redo all to make it network specific. NEC: if key is revoked, what does it mean? E//: deletion, but there is something between deletion and existing sessions. NEC: needs to be only for new sessions. VF: this should be out of scope, unfortunately allowed last meeting. delete everything related to key revocation. BT: if mobile operator cancels key, there may be problem with relying services. QC: note complete document, remove revocation in next meeting.

**Decision:** The document was **noted**.

**S3-190823 New Solution Key Lifetime**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

VF: who or what is deriving the subkeys. Should be up to application. E//: need to have different keys for applications. E//: applications are per application functions. VF: then only option 1 is sensible. Because key is going to change. BT: separate keys for applications, with individual lifetime. VF: out of scope, note it. we don't know how keys are being used. Nokia: come back to this when solution is decided, so there is no terminology confusion. QC: req. of derived keys shall not exceed anchor key lifetime. decision for option 1 is there, so note.

**Decision:** The document was **noted**.

**S3-190836 Modification of user identity in solution 2 and solution 3**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: ZTE Corporation, Nubia*

**Discussion:**

Orange: it is not user identity but SUPI, or potentially SUCI. Propose to note, consider this globally. QC: agree with Orange.

**Decision:** The document was **noted**.

**S3-190842 Solution 15 editorials**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

QC: least significant 256 bits. EMSK is potentially reused. May be revealed. EN: it is FFS whether a derived key is to be used. DCM: KAKMA derived from EMSK, EN: how to derive KAKMA is FFS.

**Decision:** The document was **revised to S3-190932**.

**S3-190932 Solution 15 editorials**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

(Replaces S3-190842)

**Decision:** The document was **approved**.

**S3-190843 Solution 15 comment on the application keys**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

C: K should be K\_NAF in GBA. VF: needs rewording. TS describes. Discussed offline.

**Decision:** The document was **revised to S3-190933**.

**S3-190933 Solution 15 comment on the application keys**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

(Replaces S3-190843)

**Decision:** The document was **approved**.

**S3-190701 Evaluation of solution 4**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Huawei, Hisilicon*

**Discussion:**

VF: need more evidence to accept the evaluation. Orange: not ready, not it. VF: note all the evaluations. E//: how should this be done. Orange: solutions are not ready, there are still Ens. Too early for evaluation. VF: evaluation is not proper. E//: ok with this comment, but need to establish way of working. VF: when there are fewer key issues added, then is the right time. Chair: need more technical details to achieve the evaluation. TNO: is there a place to look for good examples. VF: example LTKUP

**Decision:** The document was **noted**.

**S3-190806 Evaluation of solution 2**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

VF: not addressing all key issues NEC: this was not trying to full solution, so acceptable except for small items. QC: impact of PANA is quite big. Load on network authentication. No comparison on overhead. EAP AKA' has to be supported at home operator, so this needs to be added. VF: if we put this in, then the rest might not get done. Nokia: this is solution specific, so not the summary, need to define evaluation criteria. Orange: EN: this evaluation is not complete, add points by QC. VF: not enough content in section 4, hard to identify what to evaluate against. VF: object to whole document. QC: also note, come back at next meeting. Orange: remove advantages, be more neutral. BT: no supporting this paragraph. E//: what technical argument against second paragraph. QC: solution doesn't describe impact of PANA, so difficult to see impact. E//: how to improve. Note

**Decision:** The document was **noted**.

**S3-190808 Evaluation of solution 3**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Decision:** The document was **noted**.

**S3-190822 Conclusion to Solution #14**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

Orange: still ed notes in solution, so note

**Decision:** The document was **noted**.

**S3-190844 Solution 15 evaluation**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

**Discussion:**

change to figure ok, VF: remove second sentence after ed note. VF: oppose evaluation section inclusion. BT: support the last paragraph of evaluation section. VF: evaluation criteria are not there yet. Orange: evaluation criteria are required only for final evaluation. VF: against what use cases. section 4 is missing. Orange: would be ok if evaluation criteria are available in the beginning. Nokia: solution specific evaluation should be focussed on key issue only. CMCC: keep evaluation here, and do overall evaluation in section 7. Orange: need to deal with partial solutions. DCM: show which issues are solved and why. Keep comparisons to other solutions out. NEC: missing impact. Orange: add impact and advantages. Orange: need a way forward discussion.

NEC supports keeping conclusion, Apple as well. VF: second para deleted due to preference for one option. Orange: last paragraph, remove last part.

**Decision:** The document was **revised to S3-190935**.

**S3-190935 Solution 15 evaluation**

 *Type: pCR For: Approval
 33.835 v0.3.0
 Source: Ericsson*

(Replaces S3-190844)

**Decision:** The document was **approved**.

**S3-190923 draft TR 33.835**

 *Type: draft TR For: Approval
 33.835 v0.4.0
 Source: China Mobile*

**Decision:** The document was **approved**.

**S3-190934 Way forward on evaluations for FS\_AKMA**

 *Type: discussion For: Endorsement
 Source: ORANGE*

**Decision:** The document was **endorsed**.

### 5.6 Study on evolution of Cellular IoT security for the 5G System (FS\_CIoT\_sec\_5G) (Rel-16)

**S3-190611 Reply LS on authentication of group of IoT devices**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: S1-190501*

**Discussion:**

Not in scope of this meeting - postponed to next SA3 plenary

**Decision:** The document was **postponed**.

**S3-190784 Acknowledging the multiple possible mobility solutions for CP small data**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **approved**.

**S3-190815 Evaluation to Solution #3 ‘Security solution for MO SMS at AMF re-allocation’**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190816 Evaluation to Solution #4 ‘Security solution for UL small data transfer in RRC Suspend and Resume with early data transmission (EDT)’**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Ericsson*

**Discussion:**

Huawei: There are RAN issues with EDT, so propose to note

**Decision:** The document was **noted**.

**S3-190817 Evaluation to Solution #5 ‘Security solution for small data included in initial NAS signalling at mobility’**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190614 Update of Solution #6 – Use of UE Configuration Update**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: KPN N.V.*

**Abstract:**

This contribution provides an update of Solution #6 Detecting and handling signalling overload due to Malicious Applications on the UE.

**Discussion:**

Orange: MT should be used instead of UESF. EN of further evaluation needed QC: How do you provide filters for applications as they are not standardised - add an EN of this. Gemalto: Issue with the figure of UE - taken

**Decision:** The document was **noted**.

**S3-190661 Deleting EN on the usage of per-gNB and per-UE counters for solution #7 “protecting gNB from RRC DoS attack”**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

**Discussion:**

Orange: If it is left for implementation, then how does your solution work. Need text like thresholds are supported, values are for configurations.

**Decision:** The document was **revised to S3-191025**.

**S3-191025 Deleting EN on the usage of per-gNB and per-UE counters for solution #7 “protecting gNB from RRC DoS attack”**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

(Replaces S3-190661)

**Discussion:**

Check with orange and then approved without being further seen

**Decision:** The document was **approved**.

**S3-190662 Delete the EN related to the “AttackInformationNotification” message**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: Can one UE sabotage the context of another UE by replaying a message. The discussion related to evaluation and will be brought later

**Decision:** The document was **approved**.

**S3-190792 Security protection of small data at idle mode mobility**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **approved**.

**S3-190800 Adding an evaluation to solution #9 in TR 33.861**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

**Discussion:**

Huawei: Add EN on whether small data goes in Reg Request

**Decision:** The document was **revised to S3-191032**.

**S3-191032 Adding an evaluation to solution #9 in TR 33.861**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

(Replaces S3-190800)

**Decision:** The document was **approved**.

**S3-190785 Resolving the editor’s note in solution #10 in TR 33.861**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **approved**.

**S3-190786 Adding an evaluation to solution #10 in TR 33.861**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

**Discussion:**

Huawei: Add EN on whether small data goes in Reg Request

**Decision:** The document was **revised to S3-191033**.

**S3-191033 Adding an evaluation to solution #10 in TR 33.861**

 *Type: pCR For: Approval
 33.861 v0.3.0
 Source: Qualcomm Incorporated*

(Replaces S3-190786)

**Decision:** The document was **approved**.

**S3-190717 Update to solution#12"DDoS attack mitigation in CIoT"**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **approved**.

**S3-190603 Solution proposal for FS\_CIoT\_sec\_5G key issue #1 and #2**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Philips International B.V.*

**Discussion:**

Huawei: Cryptographic strength of the method need evaluation - agreed to remove evaluation and add EN of strength evaluations. Ericsson: Buffering of data at receiver is needed. EN added on this.

**Decision:** The document was **revised to S3-191027**.

**S3-191027 Solution proposal for FS\_CIoT\_sec\_5G key issue #1 and #2**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Philips International B.V.*

(Replaces S3-190603)

**Decision:** The document was **approved**.

**S3-190704 Solution to identify misbehaving UEs**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

**Discussion:**

Orange: Add EN on what kind of UE behaviour information is collected. Huawei: think it is more in scope of SA2. Ericsson: EN on privacy of collecting information

**Decision:** The document was **revised to S3-191028**.

**S3-191028 Solution to identify misbehaving UEs**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

(Replaces S3-190704)

**Decision:** The document was **approved**.

**S3-190705 Solution to Mitigate DDoS Attack based on RAN**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: Can UE send random junk effect the analysis but positioning the blacklist. Huawei: UEs not added immediately. QC :Add EN - how to identify the UE is FFS - was proposed and accepted. Vodafone: Blacklist detection report must not classify a non-mis-behaving UE as mis-behaving - also how to you get off blacklist. Huawei: SF create the list - Vodafone: two ENs one on removal and on GUTI re-use. Ericsson: EN on privacy

**Decision:** The document was **revised to S3-191029**.

**S3-191029 Solution to Mitigate DDoS Attack based on RAN**

 *Type: pCR For: Approval
 33.861 v0.4.0
 Source: Huawei, Hisilicon*

(Replaces S3-190705)

**Decision:** The document was **approved**.

**S3-190706 Conclusion for KDF negotiation for 5G System Security**

 *Type: pCR For: Approval
 33.808 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **revised to S3-190723**.

**S3-191026 draft TR 33.861**

 *Type: draft TR For: Approval
 33.861 v0.5.0
 Source: Ericsson*

**Decision:** The document was **approved**.

### 5.7 Study on the security of the Wireless and Wireline Convergence for the 5G system architecture (FS\_5WWC\_SEC) (Rel-16)

**S3-190745 New KI: N3GPP Key Hierarchy**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Ericsson*

**Discussion:**

Huawei: not needed, no new access type defined in SA2. E//: problem should be studied. ZTE: TNAP is out of scope for 3GPP, so why study it. Nokia: support this requirement, but some parts too solution specific. Huawei: needs to be more generalized, delete solution specifics. Orange: requirement is strange. add EN: req needs to be reworded. ZTE: description for key separation seems to be for authentication, why is it needed? Nokia: for encryption. ZTE: ed note to req section. Huawei: new ed note to threat: purpose needs to be clarified. TIM comment on title, is key separation. on security threat: not self-contained. on requirements: it is already like this. BT support this. TIM: prefer to keep this out until it is phrased properly. E//: have note on scope of this issue - taken offline

**Decision:** The document was **revised to S3-191012**.

**S3-191012 New KI: N3GPP Key Hierarchy**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Ericsson*

(Replaces S3-190745)

**Decision:** The document was **approved**.

**S3-190746 New Solution: New access type distinguisher for N3GPP**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Ericsson*

**Discussion:**

TIM: what is meant by optional. E//: evaluation can go away. Huawei: solution not needed

**Decision:** The document was **noted**.

**S3-190747 New Solution: Key separation for untrusted and trusted access**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Ericsson*

**Discussion:**

Same issue as 746 at initial proposal. Re-discussed one key issue in S3-191012 was approved. BT: some keys need to be included. ZTE: Add EN on whether TNAP is in scope. Huawei: Add EN on whether this addresses KI is FFS. In figure remove all except trusted.

**Decision:** The document was **revised to S3-191030**.

**S3-191030 New Solution: Key separation for untrusted and trusted access**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Ericsson*

(Replaces S3-190747)

**Decision:** The document was **approved**.

**S3-190748 New Solution: SUCI deconcealment for the FN-RG**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Ericsson*

**Discussion:**

Huawei: key issue 11 and 12 have no requirements, so what is the solution about. Nokia: NAS SMC in step 8. Gateway needs to support some sort of NAS. E//: yes. Huawei: note, because no requirements. TIM: first requirements, then solution. Note.

**Decision:** The document was **noted**.

**S3-190877 Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN)**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN)

**Discussion:**

ZTE: out of scope for SA3. Nokia: SA2 has a note in 7.1.3.5.1 of SA2. Huawei: add ed note: whether this in scope of R16. Huawei: key hierarchy in issue details is like solution. Generalize. TIM: threats are missing. E//: may lead to architectural or service requirements. Nokia: make it architectural requirement, no threats

**Decision:** The document was **revised to S3-191013**.

**S3-191013 Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN)**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190877)

**Decision:** The document was **approved**.

**S3-190878 Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN)**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN)

**Discussion:**

ZTE: same question as 877, add same ed note. Orange: is this architecture agreed? Nokia: yes.

**Decision:** The document was **revised to S3-191014**.

**S3-191014 Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN)**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190878)

**Decision:** The document was **approved**.

**S3-190710 Add content to Introduction clause**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Discussion:**

Nokia: editorials. Ed note: needs to be fixed. Orange: not in this shape. Issues with roaming. Take it next meeting.

**Decision:** The document was **noted**.

**S3-190709 Add content to section 4**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Discussion:**

Orange: same issues. Work for next meeting. Start email discussion on these topics.

**Decision:** The document was **noted**.

**S3-190713 Delete EN for solution #3**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Discussion:**

Nokia: first change: shall-> may? Huawei: bullet 1 and 2 had ed notes, but we don't know how it could be addressed. Orange: relates to authentication, keep shall. Nokia: as well. E//: why conclude this to normative, still time to do this in study phase. Huawei: SA2 has not concluded yet. E//: may be bring this for next meeting. Orange: note this contribution. TIM: also suggest to note, there is not clear there is a normative phase.

**Decision:** The document was **noted**.

**S3-190714 Add evaluation to solution #3**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Discussion:**

related to previous, Huawei proposes to note this and the 715, 716 and 712

**Decision:** The document was **noted**.

**S3-190715 Delete EN for solution 5**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **withdrawn**.

**S3-190716 Add evaluation to solution 5**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **withdrawn**.

**S3-190712 Conclusion on KI#1**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **withdrawn**.

**S3-190875 Removal of Editor’s Note in Solution#6**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Lenovo, Motorola Mobility*

**Abstract:**

This document proposes to resolve the Editor’s Note in Solution#6

**Decision:** The document was **noted**.

**S3-190711 Add content to section 4**

 *Type: pCR For: Approval
 33.807 v0.3.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **withdrawn**.

**S3-191015 draft TR 33.807**

 *Type: draft TR For: Approval
 33.807 v0.4.0
 Source: Huawei*

**Decision:** The document was **approved**.

### 5.8 Study on Security Aspects of PARLOS (FS\_PARLOS\_Sec) (Rel-16)

**S3-190615 False base station key issue for RLOS P-CR**

 *Type: pCR For: Agreement
 33.815 v0.3.0
 Source: SPRINT Corporation*

**Discussion:**

Orange & QC: Don't feel that this key issue is appropriate - this may be brought back but would need requirements

**Decision:** The document was **noted**.

**S3-190616 Reduced confidentiality protection key issue for RLOS P-CR**

 *Type: pCR For: Agreement
 33.815 v0.3.0
 Source: SPRINT Corporation*

**Discussion:**

Ericsson: very similar key issue already. Orange: Not clear can be solved. QC: Not clear this is a suitable key issue.

**Decision:** The document was **noted**.

**S3-190617 Fraud controls bypassed key issue for RLOS P-CR**

 *Type: pCR For: Agreement
 33.815 v0.3.0
 Source: SPRINT Corporation*

**Discussion:**

Orange: IMEI is not an identifier of the UE. Ericsson: Why is this a different to normal use cases. Sprint: Maybe not clear what we are trying to achieve. BT: Support this going forward. QC: Fraud control mechanism is not standardised. Sprint: These were all brought up in SA3 so have been submitted for discussion. Orange: proposal to remove the 2nd sentence as there is no concept of HPLMN. Vodafone: The IMEI cannot be checked in the normal way. QC: Disputed that the IMEI cannot be checked in the normal way. Ericsson: Need to be careful about having a list of attacks. This may be brought back but would need requirements

**Decision:** The document was **noted**.

**S3-190781 Proposed evaluation for Solution #1 AS and NAS security for RLOS services**

 *Type: pCR For: Approval
 33.815 v0.3.0
 Source: Qualcomm Incorporated*

**Discussion:**

Add EN about further evaluation if further key issues. Remove emergency calls .

**Decision:** The document was **revised to S3-191010**.

**S3-191010 Proposed evaluation for Solution #1 AS and NAS security for RLOS services**

 *Type: pCR For: Approval
 33.815 v0.3.0
 Source: Qualcomm Incorporated*

(Replaces S3-190781)

**Decision:** The document was **approved**.

**S3-190782 Proposed evaluation for Solution #2 AS and NAS security based on the emergency call procedures**

 *Type: pCR For: Approval
 33.815 v0.3.0
 Source: Qualcomm Incorporated*

**Discussion:**

There were objections to the proposed text.

**Decision:** The document was **noted**.

**S3-190783 Proposed update for Solution #2 AS and NAS security based on the emergency call procedures**

 *Type: pCR For: Approval
 33.815 v0.3.0
 Source: Qualcomm Incorporated*

**Discussion:**

Change a 'sh' to 'c'.

**Decision:** The document was **revised to S3-191011**.

**S3-191011 Proposed update for Solution #2 AS and NAS security based on the emergency call procedures**

 *Type: pCR For: Approval
 33.815 v0.3.0
 Source: Qualcomm Incorporated,Lenovo*

(Replaces S3-190783)

**Decision:** The document was **approved**.

**S3-190868 Solution Evaluations and Conclusion on KI#1**

 *Type: pCR For: Approval
 33.815 v0.3.0
 Source: Lenovo, Motorola Mobility*

**Abstract:**

This document provides the evaluations to the solutions and a conclusion for KI#1.

**Discussion:**

Merge the first clause into the S3-191010 - second part is not accepted - conclusion not accepted

**Decision:** The document was **merged**.

**S3-191023 draft TR 33.815**

 *Type: draft TR For: Approval
 33.815 v0.4.0
 Source: Sprint*

**Decision:** The document was **approved**.

### 5.9 Study on 5G security enhancement against false base stations (FS\_5GFBS) (Rel-16)

**S3-190669 New security requirement against tampering of RRCResumeRequest message**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: Why do we need to protect this? Huawei: There is the chance to protect this message. NEC and Samsung were supportive of the requirement. Ericsson and QC are not clear that the threats are sufficient to require a change. It was agreed to add an EN to capture that the security threats are not clear. The changes to the key issue details were agreed. The addition of the requirement was taken offline.

**Decision:** The document was **revised to S3-190936**.

**S3-190936 New security requirement against tampering of RRCResumeRequest message**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190669)

**Decision:** The document was **merged**.

**S3-190667 Protection of RRSResumeCause**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **noted**.

**S3-190670 New security requirement against replay of RRCResumeRequest message**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Qualcomm: It is not clear that the requirement belongs to the false base station. Huawei: It will be treated under one agenda item or another. Ericsson: Wanted the requirement to have the addition of not putting the UE out of sync with the network. Qualcomm: concern that this does not fit into the false base station work. It was taken offline to decide which study item that this work can be placed under. EN on alignment of threat and requirement.

**Decision:** The document was **revised to S3-190937**.

**S3-190937 New security requirement against replay of RRCResumeRequest message**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190670)

**Decision:** The document was **revised to S3-190997**.

**S3-190997 New security requirement against replay of RRCResumeRequest message**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190937)

**Decision:** The document was **approved**.

**S3-190668 RRCResume replay protection**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Vodafone wanted a EN on backwards compatibility issues for both UE and network - this was agreed. Ericsson raised a concern with the solution that it does not work. NEC and Qualcomm also feel that the solution does not satisfy the requirement.

**Decision:** The document was **noted**.

**S3-190829 KI#1 in TR 33.809 - new solution with network controlled RRC Reject message**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

NEC: What is the impact of the unprotected RRCReject? NEC were also not convinced the solution work. BT: Did not understand why some networks did not need RRCReject. Huawei: Feel that this solution is a violation of RAN procedures. Qualcomm: Not clear on the RAN impacts. Orange: RAN impact is RRCReject cannot be sent as it is never sent after security activation.

**Decision:** The document was **noted**.

**S3-190834 Adding evaluation for Solution #1**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Apple Computer Trading Co. Ltd*

**Discussion:**

Orange: This solution can be done with the current specification as a configuration of the network. It was not clear to Ericsson that this was only a configuration from the description of the solution. An editor's note along the following lines will be added 'The above text needs to be modified to be clarify that the above solution is a network configuration. '

**Decision:** The document was **revised to S3-190938**.

**S3-190938 Adding evaluation for Solution #1**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Apple Computer Trading Co. Ltd*

(Replaces S3-190834)

**Decision:** The document was **approved**.

**S3-190831 KI#2 in TR 33.809 – updated details (clean-up)**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

Qualcomm: Do not understand why non-public networks are mentions. Orange: Do not want the inclusion on the text for non-public network. It was agreed to remove the non-public network text and this results in a couple of new proposed references being not added.

**Decision:** The document was **revised to S3-190939**.

**S3-190939 KI#2 in TR 33.809 – updated details (clean-up)**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

(Replaces S3-190831)

**Decision:** The document was **approved**.

**S3-190798 Changing the security requirement for KI #2**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Qualcomm Incorporated*

**Discussion:**

Samsung: Add in all RRC states to the requirements. Ericsson: Change SIBs to SI.

**Decision:** The document was **revised to S3-190940**.

**S3-190940 Changing the security requirement for KI #2**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190798)

**Decision:** The document was **approved**.

**S3-190676 Cell Authenticated Access for fake base station detection**

 *Type: pCR For: (not specified)
 33.809 v0.2.0
 Source: Intel Mobile Communications*

**Discussion:**

Qualcomm: What does a UE do before it has connected the network. Intel: Add an Editor's note to capture this. ZTE: Why is the private key sent to the UE. Intel: This is a mistake and should be removed. Qualcomm: Does this solution require sharing a private key across all elements in the network. An editor's note was added related to this. Orange: It is not clear how all the needed keys get provisioned - this is fundamental to the solution. BT: Won't this introduce a false base station to prevent the UE attaching to real base station by sending broadcast messages with a wrong signature. Orange, DT and Qualcomm felt that there were too many important issues that are unclear with the solution to accept the solution at this time.

**Decision:** The document was **noted**.

**S3-190832 KI#2 in TR 33.809 – new solution for tamper resistant SI messages**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

Orange: Feels that this proposal is similar to the previous one in details. Ericsson: use this solution as a way of gathering the issues on signing message. Intel, Samsung, Interdigital and Apple support the inclusion of contribution. There was discussion on whether there could be a way of capturing the impact of signed SI. There was general agreement that capturing the general issue of signing SIs would provide a mechanism to make progress on the false base station study. A revision was allocated for the creation (probably of an Annex) that will enable studying the impacts of signing broadcast messages.

**Decision:** The document was **revised to S3-190941**.

**S3-190941 KI#2 in TR 33.809 – new solution for tamper resistant SI messages**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

(Replaces S3-190832)

**Decision:** The document was **approved**.

**S3-190835 Adding evaluation for Solution #2**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Apple Computer Trading Co. Ltd*

**Discussion:**

Orange: this is not a disadvantage as the solution does not claim to solve this issue. Samsung supports this. Ericsson and Apple believe that the disadvantage should be kept. It was proposed to not have an evaluation at this time as there is still a fundamental. The other changes were agreed.

**Decision:** The document was **revised to S3-190942**.

**S3-190942 Adding evaluation for Solution #2**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Apple Computer Trading Co. Ltd*

(Replaces S3-190835)

**Decision:** The document was **approved**.

**S3-190865 Evaluation of Solution #2**

 *Type: pCR For: (not specified)
 33.809 v0.2.0
 Source: Samsung*

**Discussion:**

E//: need to resolve ed note first

**Decision:** The document was **noted**.

**S3-190630 5GFBS-solution Using symmetric algorithm with assistance of USIM and home network**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: ZTE Corporation*

(Replaces S3-190155)

**Discussion:**

Orange: Which entity is the one who provisions the USIM. ZTE: Visited network provision the USIM. Orange: No way. ZTE: The provisioning procedure can be run by the home network. Interdigital: The initial provisioning well not work.

**Decision:** The document was **noted**.

**S3-190776 Certificate based solution against false base station**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Apple Computer Trading Co. Ltd*

**Discussion:**

Orange, Qualcomm and DT all felt that the solution needs to wait until the new 'Annex' on signature was done.

**Decision:** The document was **noted**.

**S3-190833 ID based solution against false base station**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Apple Computer Trading Co. Ltd*

**Discussion:**

Orange, Qualcomm and DT all felt that the solution needs to wait until the new 'Annex' on signature was done.

**Decision:** The document was **noted**.

**S3-190866 Solution for AS security during RRC Idle mode**

 *Type: pCR For: (not specified)
 33.809 v0.2.0
 Source: Samsung*

**Discussion:**

Proposal to update the title and the introduction - this was agreed. Qualcomm: An EN on what happens at Location Update.

**Decision:** The document was **revised to S3-190943**.

**S3-190943 Solution for AS security during RRC Idle mode**

 *Type: pCR For: -
 33.809 v0.2.0
 Source: Samsung*

(Replaces S3-190866)

**Decision:** The document was **approved**.

**S3-190635 Updating Key issue #3 for Network detection of nearby false base station**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes an update to key issue #3 in TR 33.809.

**Discussion:**

Huawei supports the contribution. Ericsson and Qualcomm think that the text is already covered by KI#4. Some of the proposed text was not included to remove overlap.

**Decision:** The document was **revised to S3-190944**.

**S3-190944 Updating Key issue #3 for Network detection of nearby false base station**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

(Replaces S3-190635)

**Decision:** The document was **approved**.

**S3-190825 KI#3 in TR 33.809 - updates to updates to details and threats**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

Huawei supports the contribution.

**Decision:** The document was **approved**.

**S3-190826 KI#3 in TR 33.809 - updates to requirements**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

The proposal was changed to make it acceptable.

**Decision:** The document was **revised to S3-190945**.

**S3-190945 KI#3 in TR 33.809 - updates to requirements**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

(Replaces S3-190826)

**Decision:** The document was **approved**.

**S3-190828 KI#3 in TR 33.809 - conclusion on second requirement (reactive action)**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

NEC: Not clear why the information cannot be supplied to UE - overall too early to introduce. Huawei also believe it is too early to introduce the conclusions.

**Decision:** The document was **noted**.

**S3-190654 Notifying cell information to the network after authentication procedure failure**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes a new solution.

**Discussion:**

Interdigital: Feel that this is an attack scenario on the UE and an EN should be added to include this. Qualcomm: Two Ens are proposed - it is ffs whether cell re-selection finds a cell of the same PLMN and what happens if authentication failure happens in re-selected cell. Huawei: Would like an EN about step 8 - this was agreed. There were concerns that this signalling does not work as it seems to require new signalling to the home network.

**Decision:** The document was **revised to S3-190998**.

**S3-190998 Notifying cell information to the network after authentication procedure failure**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

(Replaces S3-190654)

**Discussion:**

Issue about HPLMN is not resolved. QC: Network based detection so far has been in the serving network. NEC: Will make the solution only apply for the non-roaming case.

**Decision:** The document was **revised to S3-191006**.

**S3-191006 Notifying cell information to the network after authentication procedure failure**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

(Replaces S3-190998)

**Decision:** The document was **noted**.

**S3-190674 Notifying cell information to the network when the UE determines that the network fails the authentication procedure**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

Reporting false base station to the network.

**Decision:** The document was **withdrawn**.

**S3-190660 Network detection of false base station from UE measurement reports**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Nokia*

**Discussion:**

Huawei: This can be done with current signalling. Orange: remove the evaluation - this was agreed. Pro-active and instructing the UE are removed.

**Decision:** The document was **revised to S3-190946**.

**S3-190946 Network detection of false base station from UE measurement reports**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Nokia*

(Replaces S3-190660)

**Decision:** The document was **approved**.

**S3-190665 Avoiding UE connecting to fake base station during HO**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

An EN saying roughly "the details of how the UE hands over to the false base station need to be clarified". It was agreed to delete the evaluation.

**Decision:** The document was **revised to S3-190947**.

**S3-190947 Avoiding UE connecting to fake base station during HO**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190665)

**Decision:** The document was **approved**.

**S3-190666 Measurement report requirement for the case when the UE in RRC-IDLE & RRC-INACTIVE**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **merged**.

**S3-190671 Measurement Report Requirement When UE in RRC-CONNECTED**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **merged**.

**S3-190827 KI#3 in TR 33.809 - new solution for enriched measurement reports**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

One EN on UE power consumption will be added and this is merged with S3-190671 and S3-190666

**Decision:** The document was **revised to S3-190985**.

**S3-190985 KI#3 in TR 33.809 - new solution for enriched measurement reports**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson,Huawei*

(Replaces S3-190827)

**Decision:** The document was **approved**.

**S3-190733 New requirement for Authentication relay attack**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: Concern that the attack is not so serious and the requirement is too strongly worded. Orange: Proposal for EN - "There should be means to mitigate the auth relay attack caused by a false base station".

**Decision:** The document was **revised to S3-190986**.

**S3-190986 New requirement for Authentication relay attack**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190733)

**Decision:** The document was **approved**.

**S3-190837 Improvement to key issue #5**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: ZTE Corporation, Nubia*

**Discussion:**

Both Orange and Huawei felt that the text was not related to this key issue and hence should not be included here. It was possible that there may a different key issue proposed by the text.

**Decision:** The document was **noted**.

**S3-190655 Protection of UE configuration against false base station**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes a new solution.

**Discussion:**

Huawei: UE is attaching to a network for an unauthenticated emergency call and hence does not trust the network. Apple: Needs a key issue to be included. Qualcomm: It is a solution

**Decision:** The document was **noted**.

**S3-190673 Handling of UE configuration update by a fake base station**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

Protecting UE configuration from false base station.

**Decision:** The document was **withdrawn**.

**S3-190734 New solution for Authentication relay attack**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Lenovo: Victim UE and malicious UE need to be in the same PLMN. Ericsson and Samsung: Proposed EN "Details of how UE location info is used and granularity and secured from false base station attack . Samsung: EN proposal "How the UE obtains the location is FFS". "Qualcomm: Proposal for EN "How the solution addresses already registered UE is FFS" . BT: Need to take privacy aspects into account - an EN was added.

**Decision:** The document was **revised to S3-190987**.

**S3-190987 New solution for Authentication relay attack**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190734)

**Decision:** The document was **approved**.

**S3-190838 Detection of false relay base station by UE**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: ZTE Corporation, Nubia*

**Discussion:**

There was lots of discussion on whether the proposed solution work as described and it was also not clear how it fitted the key issue

**Decision:** The document was **noted**.

**S3-190870 Solution on Authentication Relay Attack**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Lenovo, Motorola Mobility*

**Abstract:**

This paper provides a solution on key issue Key Issue #5: Mitigation against the authentication relay attack.

**Decision:** The document was **merged**.

**S3-190663 Propose a new KI and security requirement for spoofing paging messages**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

NEC: Do not feel that there is a legitimate security threat here. Ericsson: Have sympathy for the NEC view. Orange: do not agree with key issue being accepted

**Decision:** The document was **noted**.

**S3-190664 Protection for Incoming Paging Message Based on Stored Security Context**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Related key issue was not accepted

**Decision:** The document was **noted**.

**S3-190675 Key Issue for Fake Base Station**

 *Type: pCR For: (not specified)
 33.809 v0.2.0
 Source: Intel Mobile Communications*

**Discussion:**

It was felt that the proposals in this key issue are already covered by another contribution

**Decision:** The document was **noted**.

**S3-190793 Protection against Man-in-the-Middle false base station attacks**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190381)

**Discussion:**

Huawei proposed to make the requirement a should - this was not accepted. Ericsson: Do not want to accept the requirement. This view was support by Samsung and NEC. The key issue details and security requirements were not challenged. Discussion on the requirement was taken offline.

**Decision:** The document was **revised to S3-190988**.

**S3-190988 Protection against Man-in-the-Middle false base station attacks**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190793)

**Discussion:**

Ericsson: want to note the document as it is an evaluation contribution. Orange: Support the contribution. The discussion was concluded by agreeing to have no security requirement as this meeting.

**Decision:** The document was **revised to S3-191021**.

**S3-191021 Protection against Man-in-the-Middle false base station attacks**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190988)

**Decision:** The document was **approved**.

**S3-190830 New annex in TR 33.809 - summary of PWS security study**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: Ericsson*

**Discussion:**

There was much discussion on whether to include the conclusion from PWS study in the FBS TR.

**Decision:** The document was **noted**.

**S3-190636 Solution for preventing UE camping on false base station during Idle mode**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes a solution for preventing UE from camping on false base station.

**Decision:** The document was **withdrawn**.

**S3-190960 draft TR 33.809**

 *Type: draft TR For: Approval
 33.809 v0.3.0
 Source: Apple*

**Decision:** The document was **approved**.

**S3-190989 References to TR 33.809**

 *Type: pCR For: Approval
 33.809 v0.2.0
 Source: BT*

**Discussion:**

There will be reference to the previous work in the introduction. Orange was objecting to the approval of the document but this was sufficient support for approval.

**Decision:** The document was **approved**.

### 5.10 Study of KDF negotiation for 5G System Security (FS\_5GS\_KDF) (Rel-16)

**S3-190723 Conclusion for KDF negotiation for 5G System Security**

 *Type: pCR For: Approval
 33.808 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190706)

**Discussion:**

Ericsson: remove 1st and 3rd sentence . NCSC 2nd sentence needs modification to remove SA3.

**Decision:** The document was **revised to S3-190957**.

**S3-190957 Conclusion for KDF negotiation for 5G System Security**

 *Type: pCR For: Approval
 33.808 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190723)

**Decision:** The document was **approved**.

**S3-190958 draft TR 33.808**

 *Type: draft TR For: discussion
 33.808 v0.3.0
 Source: Huawei*

**Decision:** The document was **approved**.

### 5.11 Study on Security aspects of Enhancement of Network Slicing (FS\_eNS\_SEC) (Rel-16)

**S3-190609 Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: InterDigital, Inc.*

**Abstract:**

A new solution for Slice Specific Authentication and Authorization when UE is registering in the same AMF in the same serving PLMN over both 3GPP and non-3GPP accesses

**Discussion:**

Huawei: regarding Slice authentications, you want to check whether this has been done on 3GPP or non-3GPP. Interdigital: We have opened up security details of the SA2 solution. Nokia: SA2 do not differentiate between accesses but you do. Interdigital: We assume that UE may register on both access types. Nokia: That scenario is already covered. Ericsson: Further information is needed on why there is a dependency on different accesses captured agreed for EN. Nokia: Another EN on aligning call flow and terminology with SA2. NEC: we have agreed to use slice or slice-specific authentication

**Decision:** The document was **revised to S3-191002**.

**S3-191002 Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: InterDigital, Inc.*

(Replaces S3-190609)

**Decision:** The document was **approved**.

**S3-190697 Amendment to solution #2**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

**Discussion:**

Ericsson: What is the role of the SAF - this is not part of the SA2 solution. Huawei: Proposing to change SAF to AAA proxy. NEC: Steps we are adding are incorrect. Nokia The open issue on nesting needs to be solved by SA2 and CT1. NEC: Agree with Nokia - as it is not aligned with SA2 and hence broken. Huawei: It is not broken. Nokia, QC and NEC say it should not go in.

**Decision:** The document was **noted**.

**S3-190692 Discussions on solutions to AMF key separation**

 *Type: discussion For: Discussion
 33.813 v..
 Source: Huawei, HiSilicon*

**Discussion:**

Discussion only - comments will be on solution proposals

**Decision:** The document was **noted**.

**S3-190693 AMF key separation solution 1**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

**Discussion:**

Nokia: Fast re-authentication has been discussed previously. An EN will be added to note this. Ericsson: this still involves of going to the HPLMN so an EN on what are the advantages. NEC: Mutually exclusive slices did not conclude in Rel-16 - there will be an offline check on whether we need an LS to get official confirmation

**Decision:** The document was **noted**.

**S3-190694 AMF key separation solution 2**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **noted**.

**S3-190695 AMF key separation solution 3**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **noted**.

**S3-190799 KAMF separation using a standalone SEAF**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **noted**.

**S3-190814 Solution for key separation based on slice authentication keys**

 *Type: pCR For: Approval
 33.813 v0.3.0
 Source: Ericsson*

**Decision:** The document was **noted**.

**S3-190696 Discussion on provisioning security features for a network slice**

 *Type: discussion For: Discussion
 33.813 v..
 Source: Huawei, HiSilicon*

**Discussion:**

Motivating solutions in other papers

**Decision:** The document was **noted**.

**S3-190698 Amendment to solution #3**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

**Discussion:**

Nokia: Policy can be configured in the SMF. Huawei: Configuring a slice has all the possibilities but just want to have a small set of things that can be configured. This is done through management plane. Nokia: These details should be provided in the solution. ZTE: Why is there secondary authentication for a slice. Huawei: You have a choice to use this at PDU session set-up. TI: Does not understand the link between secondary and slice authentication. BT: Clarity needed on what can be done dynamically and what is fixed in the network. The slices needs to have something unique about them, otherwise what is the point. Offline discussion concluded on revision of a sentence.

**Decision:** The document was **revised to S3-191007**.

**S3-191007 Amendment to solution #3**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

(Replaces S3-190698)

**Decision:** The document was **approved**.

**S3-190867 Privacy for Slice Authentication**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Lenovo, Motorola Mobility*

**Abstract:**

This paper introduces a solution on Key Issue #4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization.

**Discussion:**

Orange: Concerned about the binding between the S-NSSAI and public leaks information about the networks deployment. It was agreed to remove that binding. QC: Privacy is EAP method specific and hence there is no reason to have the solution. Lenovo: There is a key issue for this so we should study for solutions. If someone believes that the key issue is no longer valid., the they should propose removing it. Huawei: Support including the solution. Ericsson: Does this change EAP. Lenovo: Some impact on decrypting identity

**Decision:** The document was **revised to S3-191017**.

**S3-191017 Privacy for Slice Authentication**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Lenovo, Motorola Mobility*

(Replaces S3-190867)

**Discussion:**

Lenovo: Think that this a workable solution. QC raised 3 EN - identity for slice auth is in scope, problem with public key and secondary auth uses EAP.

**Decision:** The document was **revised to S3-191034**.

**S3-191034 Privacy for Slice Authentication**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Lenovo, Motorola Mobility*

(Replaces S3-191017)

**Decision:** The document was **approved**.

**S3-190738 Remove EN in 6.6.3**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Orange: Inconsistent to remove only one of the ENs as they refer to each other. Huawei: Remove the first EN as well. It was agreed.

**Decision:** The document was **revised to S3-191008**.

**S3-191008 Remove EN in 6.6.3**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190738)

**Decision:** The document was **approved**.

**S3-190739 Solution for slice specific authorization**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

Nokia: What is NSI-ID - a reference will be added to clarify this.

**Decision:** The document was **revised to S3-191009**.

**S3-191009 Solution for slice specific authorization**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, Hisilicon*

(Replaces S3-190739)

**Decision:** The document was **approved**.

**S3-190656 NSSAI protection during the RRC connection establishment procedure**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes a new solution.

**Discussion:**

ZTE: It is not clear how the security context is found. Add EN about finding the source gNB. Nokia: UE has NAS context so AMF already known, so what is actually being protected. NEC: The S-NSSAI are protected during the Service Request procedure. Huawei: Agree with Nokia. NEC: S-NSSAI is used not only for routing but also AS procedure. Qualcomm: concern about keeping state in idle and should note. There were other companies concerned about storage of state in RRC-inactive

**Decision:** The document was **noted**.

**S3-190657 NSSAI protection during the RRC connection establishment procedure**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes a new solution.

**Discussion:**

Ericsson: Issue is that the routing to an AMF is already done and doesn't this defeat the purpose of procedure. NEC: S-NSSAIs are needed for more than just AMF selection. Qualcomm: How is AMF found? NEC: with GUTI. Ericsson & Nokia: Not clear what the problem is and the why the solution is needed. NEC: Key and not AS security context is provided to the gNB. Ericsson: Not clear why the RAN needs S-NSSAI other than for AMF selection. Gemalto: Have a similar connection. NEC: S-NSSAI is contained in RRC message for purposes other than AMF selection.

**Decision:** The document was **noted**.

**S3-190791 Proposed solution for protecting the S-NSSAI for transmission at the AS layer**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Qualcomm Incorporated*

**Discussion:**

Overall the reasons for S-NSSAIs were not clear

**Decision:** The document was **noted**.

**S3-190699 Amendment to KI#6**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: Huawei, HiSilicon*

**Discussion:**

NEC: not sure the change is needed. Nokia: don’t believe change is needed. Orange, Ericsson and Qualcomm are not supportive of the changes.

**Decision:** The document was **noted**.

**S3-190771 Key issue on Granularity of isolation for slice specific security**

 *Type: pCR For: Approval
 33.813 v0.2.0
 Source: LG Electronics*

**Discussion:**

Related to key separation.

**Decision:** The document was **noted**.

**S3-190948 draft TR 33.813**

 *Type: draft TR For: Approval
 33.813 v0.3.0
 Source: Nokia*

**Decision:** The document was **approved**.

### 5.12 Study on Security of the enhancement to the 5GC location services (FS\_eLCS\_Sec) (Rel-16)

**S3-190731 pCR to TR33.814 – Text for Clause Introduction**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT*

**Discussion:**

The difference between regulatory and commercial location services was not clear and not needed in the introduction - the document will be revised to remove these terms

**Decision:** The document was **revised to S3-190898**.

**S3-190898 pCR to TR33.814 – Text for Clause Introduction**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT*

(Replaces S3-190731)

**Decision:** The document was **approved**.

**S3-190732 Text for Clause 4 Security aspects of eLCS**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT*

**Discussion:**

There was discussion on commercial location not being fully specified in Rel-15 and needs to be enhanced in Rel-16. This leads to a need to re-word 4.1 to account for this. It was agreed to remove 4.2.

**Decision:** The document was **revised to S3-190899**.

**S3-190899 Text for Clause 4 Security aspects of eLCS**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT*

(Replaces S3-190732)

**Decision:** The document was **approved**.

**S3-190729 pCR to TR33.814 - Key issue for positioning data confidentiality protection**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT*

**Discussion:**

There was general agreement on this but will be taken offline for re-wording - the revision of this will contain an EN to agree that there will be no mechanism to protect individual NAS IEs.

**Decision:** The document was **revised to S3-190900**.

**S3-190900 pCR to TR33.814 - Key issue for positioning data confidentiality protection**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT,Huawei*

(Replaces S3-190729)

**Decision:** The document was **approved**.

**S3-190719 Key Issue for encryption and integrity protection of assistance data**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

It was not clear what was missing from the Rel-15 security - this analysis would help the understanding of this key issue.

**Decision:** The document was **noted**.

**S3-190720 Key Issue for encryption and integrity protection of location data**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

This contribution overlaps with S3-190729 and will be merged into the revision of that document.

**Decision:** The document was **merged**.

**S3-190730 pCR to TR33.814 - Solution for positioning data confidentiality protection**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: CATT*

**Discussion:**

It was felt too early to conclude on this solution as there is no key issue for this yet, i.e. need to resolve whether there needs to be protection of NAS IEs when NAS security is not activated. The meeting agreed that there should not be a mechanism to protect individual NAS IEs- this will be captured by an EN in S3-190900.

**Decision:** The document was **noted**.

**S3-190721 Key Issue for privacy setting integrity between UE and home network**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Huawei, Hisilicon*

**Discussion:**

There was much discussion on whether this is a legitimate key issue. It was felt that the serving network can already determine the UE's location and hence it is not possible to prevent a serving network from using the UE's locations. Mechanisms outside the scope of standards could be useful here. A NOTE will be added to S3-190900 to try to capture this discussion - otherwise an EN will be added .

**Decision:** The document was **noted**.

**S3-190772 Key issue on UE location privacy setting**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: LG Electronics*

**Discussion:**

The same discussion as above document.

**Decision:** The document was **noted**.

**S3-190755 New KI: Privacy control in LCS**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

**Discussion:**

The word ' effective' was removed from the requirement as it is not easy to assess what is effective. 'System' was changed to '5G system' in the requirement. An EN is added to capture the open issue of who enforces the privacy.

**Decision:** The document was **revised to S3-190902**.

**S3-190902 New KI: Privacy control in LCS**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

(Replaces S3-190755)

**Decision:** The document was **approved**.

**S3-190881 Key Issue proposal on location measurement tampering for FS\_eLCS\_Sec**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Philips International B.V.*

**Abstract:**

In several 3GPP location services, the UE of which the location is to be determined performs measurements itself and sends these measurements to the network so the network can determine its location. Examples are

• OTDOA (Observed Time Difference Of Arriv

**Discussion:**

Corrections were needed to the formatting. 5.X.2 needs to be removed as that is not used for key issues in this topic. The 'etc.' is removed from security threats. It was felt that the threats could be re-written to make it clear that the ME is lying about location related data and also to include threats when location can be monitored in some way, e.g. cheaper calls from home. It was agreed to remove the requirements.

**Decision:** The document was **revised to S3-190903**.

**S3-190903 Key Issue proposal on location measurement tampering for FS\_eLCS\_Sec**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Philips International B.V.*

(Replaces S3-190881)

**Decision:** The document was **revised to S3-190959**.

**S3-190959 Key Issue proposal on location measurement tampering for FS\_eLCS\_Sec**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Philips International B.V.*

(Replaces S3-190903)

**Decision:** The document was **approved**.

**S3-190722 Solution on integrity protection of privacy setting between UE and UDM**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **noted**.

**S3-190756 New solution: Effective privacy control in LCS**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

**Discussion:**

There were several changes agreed for this contribution, namely remove effective and replace with enhanced, add sentence on steps and clarify the measurements are related to location measurements

**Decision:** The document was **revised to S3-190904**.

**S3-190904 New solution: Effective privacy control in LCS**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

(Replaces S3-190756)

**Decision:** The document was **approved**.

**S3-190751 New solution: WLAN measurements from UEs**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

**Discussion:**

It was commented that the WLAN identities can be spoofed, then there would be a lack of confidence in the data. It was agreed to add a sentence of the contribution. Editorially it is needed to decide UE or UEs in many places. Clarification on the serving network and the fact that it is for managed WLAN documents. Some of the wording will be checked offline.

**Decision:** The document was **revised to S3-190905**.

**S3-190905 New solution: WLAN measurements from UEs**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

(Replaces S3-190751)

**Decision:** The document was **approved**.

**S3-190752 New solution: Bluetooth measurements from UEs**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

**Discussion:**

same comments as to 751, so same updates

**Decision:** The document was **revised to S3-190906**.

**S3-190906 New solution: Bluetooth measurements from UEs**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

(Replaces S3-190752)

**Decision:** The document was **approved**.

**S3-190753 Update KI: TBS positioning**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190754 New solution: TBS measurements from UEs**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

**Discussion:**

VF: how to reconciliate the non-commercial nature of R15 with the statement that R15 solution is sufficient. E//: Add sentence that R15 is sufficient also for commercial LCS BT: spoofing of SSIDs is easy, similar sentence to 751

**Decision:** The document was **revised to S3-190907**.

**S3-190907 New solution: TBS measurements from UEs**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Ericsson*

(Replaces S3-190754)

**Decision:** The document was **approved**.

**S3-190718 Solution for updating key to broadcast assistance data**

 *Type: pCR For: Approval
 33.814 v0.2.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **noted**.

**S3-190901 draft TR 33.814**

 *Type: draft TR For: Approval
 33.814 v0.3.0
 Source: CATT*

**Decision:** The document was **approved**.

### 5.13 Study on security for 5G URLLC (FS\_5G URLLC\_SEC) (Rel-16)

**S3-190681 overall introduction**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **approved**.

**S3-190619 URLLC-KI UP security performance for low latency**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: ZTE Corporation*

**Discussion:**

Ericsson: Does not seem to be enough evidence from the key issue details to justify the requirement. ZTE: Details for IPsec are only example and the can be a ways to optimise performance. NEC: Does not understand the issue and support Ericsson view. Ericsson proposal to add EN to key issue details to say that further justification is required before SA3 proceeds with this key issue needed and delete the threat and requirements. Nokia: Remove the last sentence in key issue details. This proposal was accepted.

**Decision:** The document was **revised to S3-190969**.

**S3-190969 URLLC-KI UP security performance for low latency**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: ZTE Corporation*

(Replaces S3-190619)

**Decision:** The document was **approved**.

**S3-190620 URLLC-solution Enhancement of handover with Xn forwarding tunnel**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: ZTE Corporation*

**Discussion:**

Related to the key issue in S3-190969 and hence noted as no agreement to proceed on key issue.

**Decision:** The document was **noted**.

**S3-190819 New solution for security for redundant data transmission using Dual Connectivity procedures**

 *Type: pCR For: Approval
 33.825 v0.2.0
 Source: Ericsson*

**Discussion:**

Huawei: There are other contributions addressing similar solutions. Ericsson: why not have two solutions. Huawei: Concern on the details of handling of UP security policy - remove 'or other solution' to make it clear that solution #1 is used. This was agreeable. Huawei: is this an update of solution #1. Ericsson: That is a different problem to the one addressed here which is about the keys and traffic protection. Qualcomm: reference numbers are not correct - this will be corrected in revision.

**Decision:** The document was **revised to S3-190970**.

**S3-190970 New solution for security for redundant data transmission using Dual Connectivity procedures**

 *Type: pCR For: Approval
 33.825 v0.2.0
 Source: Ericsson*

(Replaces S3-190819)

**Decision:** The document was **approved**.

**S3-190631 Evaluation and text for resolving editor’s note for solution #5 in TR 33.825**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution proposes solution evaluation and text for resolving editor’s note for solution #5 in TR 33.825.

**Discussion:**

Authors agreed to merge S3-190631 and S3-190682. Ericsson: More justification of the change in keying as this is a major change to the architecture. Qualcomm: Concern that more security analysis is needed as the security model has changed. Huawei: this is a new service so we can use new solution. NEC: Concerned that the key issue is being interpreted in different ways. Ok to merge the documents with the EN on further evaluation is needed and an EN on justification for the use of new key.

**Decision:** The document was **merged**.

**S3-190682 URLLC solution5 update**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **revised to S3-190971**.

**S3-190971 URLLC solution5 update**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon,NEC*

(Replaces S3-190682)

**Decision:** The document was **approved**.

**S3-190689 Dynamic UP security policy control solution for URLLC**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

Ericson: What's new compared to now as there is some mention of dynamic. Not clear how you solve using the same policy on each leg. Huawei: the new issue is that SMF can get something from PCF. An EN saying further information on how this solution manages redundant policy.

**Decision:** The document was **revised to S3-190972**.

**S3-190972 Dynamic UP security policy control solution for URLLC**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

(Replaces S3-190689)

**Decision:** The document was **approved**.

**S3-190818 Solution #Y: Security for redundant data transmission using Dual Connectivity**

 *Type: pCR For: Approval
 33.825 v0.2.0
 Source: Ericsson*

**Discussion:**

Huawei: For solution details, more details are needed on the handling of the solution for issue #1. For issue #2, selection of SN might depend on capabilities. For issue #1, it was agreed to have an EN on the need for more details. For solution #2, the discussion was taken offline. Qualcomm: How does this relate to solution #1. Ericsson: it is an alternative to solution #1.

**Decision:** The document was **revised to S3-190973**.

**S3-190973 Solution #Y: Security for redundant data transmission using Dual Connectivity**

 *Type: pCR For: Approval
 33.825 v0.2.0
 Source: Ericsson*

(Replaces S3-190818)

**Decision:** The document was **approved**.

**S3-190685 solution1 and evaluation update**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

Ericsson: Are concerned that the text actually goes against the original proposal in the solution. It is taken offline to consider the changes and how they could be adapted to be in line with the current solution

**Decision:** The document was **revised to S3-190974**.

**S3-190974 solution1 and evaluation update**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

(Replaces S3-190685)

**Decision:** The document was **approved**.

**S3-190680 deleting the EN of solution3**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

Ericsson: concern that the UP security policy is changing. An EN on this will be added to the key issue details

**Decision:** The document was **revised to S3-190975**.

**S3-190975 deleting the EN of solution3**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

(Replaces S3-190680)

**Decision:** The document was **approved**.

**S3-190820 Correction to solution #3 ‘Security policy handling for redundant data transmission’**

 *Type: pCR For: Approval
 33.825 v0.2.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190683 evaluation of solution 3**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

Ericsson: EN has been added to the solution in an earlier document. Second sentence of evaluation was removed. Orange: Modify the existing note to make it read that further evaluation is still needed. LI EN will be removed.

**Decision:** The document was **revised to S3-190976**.

**S3-190976 evaluation of solution 3**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

(Replaces S3-190683)

**Decision:** The document was **approved**.

**S3-190679 solution 2 clarification**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

Ericsson: Add 'as described in TS 33.501 to end of new text. Evaluation text format to be corrected.

**Decision:** The document was **revised to S3-190977**.

**S3-190977 solution 2 clarification**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

(Replaces S3-190679)

**Decision:** The document was **approved**.

**S3-190678 conclusion for key issue 6**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **approved**.

**S3-190796 Conclusion on KI #6 for Study on the security for URLLC**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **noted**.

**S3-190686 conclusion for key issue 1**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

QC: not ready to make conclusion on key issue 1 for solution 5. need to resolve ed not first. Also issue with other solution. Huawei: why not? Chair: no other support, no further comments. Orange: remove all conclusions on solution 5. Huawei: get straight what means cryptographic separation. E//: note this conclusion for now. there is a new solution on key issue 1.

**Decision:** The document was **noted**.

**S3-190687 conclusion for key issue 2**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Discussion:**

E//: key issue 1 conclusion will decide what to do for all the other conclusions. Huawei: this is the question. E//: cryptographic separation discussion needs to be resolved. For these key issues not necessary in this meeting. Orange: then more contributions can eb noted. E//: other contributions will also have the same issue. E//: treat next meeting, work offline before.

**Decision:** The document was **noted**.

**S3-190677 conclusion for key issue 3**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **noted**.

**S3-190794 Conclusion on KI #3 for Study on the security for URLLC**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **noted**.

**S3-190684 conclusion for key issue 4**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **noted**.

**S3-190795 Conclusion on KI #4 for Study on the security for URLLC**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **noted**.

**S3-190797 Conclusion on KI #8 for Study on the security for URLLC**

 *Type: pCR For: Approval
 33.825 v0.3.0
 Source: Qualcomm Incorporated*

**Discussion:**

Huawei: support this contribution. E//: fine with this. Editor's note in key issue. KI needs to be aligned. BT: support this. Difficult to position this, to avoid username and password

**Decision:** The document was **approved**.

**S3-190979 draft TR 33.825**

 *Type: draft TR For: Approval
 33.825 v0.4.0
 Source: Huawei*

**Decision:** The document was **approved**.

### 5.14 Study on SECAM and SCAS for 3GPP virtualized network products (FS\_VNP\_SECAM\_SCAS) (Rel-16)

**S3-190757 Considerations on network product class when using NFV technology**

 *Type: pCR For: (not specified)
 33.818 v0.1.0
 Source: China Mobile Com. Corporation*

**Discussion:**

Taken offline to correct some editorials

**Decision:** The document was **revised to S3-190951**.

**S3-190951 Considerations on network product class when using NFV technology**

 *Type: pCR For: -
 33.818 v0.1.0
 Source: China Mobile Com. Corporation*

(Replaces S3-190757)

**Decision:** The document was **approved**.

**S3-190758 Considerations on SECAM of the virtualized network products**

 *Type: pCR For: (not specified)
 33.818 v0.1.0
 Source: China Mobile Com. Corporation*

**Decision:** The document was **revised to S3-190952**.

**S3-190952 Considerations on SECAM of the virtualized network products**

 *Type: pCR For: -
 33.818 v0.1.0
 Source: China Mobile Com. Corporation*

(Replaces S3-190758)

**Discussion:**

An EN was added

**Decision:** The document was **approved**.

**S3-190950 draft TR 33.818**

 *Type: draft TR For: Approval
 33.818 v0.2.0
 Source: China Mobile*

**Decision:** The document was **approved**.

### 5.15 Study on Security for 5GS Enhanced support of Vertical and LAN Services (FS\_Vertical\_LAN\_SEC) (Rel-16)

**S3-190862 Key issue on Alignment of the terms Private network and NPN**

 *Type: pCR For: (not specified)
 33.819 v0.2.0
 Source: Samsung*

**Discussion:**

Presented and then S3-190882 opened. Orange: OK to change term in TS 33.501. SA3 agreed that the terms private network and non-public network need to be aligned with TS 22.261.

**Decision:** The document was **noted**.

**S3-190700 Discussion on NPN authentication**

 *Type: discussion For: Endorsement
 33.819 v..
 Source: Huawei, HiSilicon*

**Decision:** The document was **revised to S3-190962**.

**S3-190962 Discussion on NPN authentication**

 *Type: discussion For: Endorsement
 33.819 v..
 Source: Huawei, HiSilicon*

(Replaces S3-190700)

**Discussion:**

Orange: Did not agree with any of the options. Huawei: Are worried that we are currently going round in circles. Orange: Prefer an option E where nothing is specified. Several other companies support this view. Qualcomm: Concerned that the scope of what we are trying to agree is not clear.

**Decision:** The document was **noted**.

**S3-190787 Proposed solution to the key hierarchy for non-public networks**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **revised to S3-190991**.

**S3-190991 Proposed solution to the key hierarchy for non-public networks**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190787)

**Decision:** The document was **approved**.

**S3-190788 Proposed addition to key issue#1.1 for standalone non-public networks**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

**Discussion:**

DCM: What to turn this into architectural reference by removing security threats and changing title of the clause to architectural. Samsung: Add EN on review after progress in stage 3

**Decision:** The document was **revised to S3-190992**.

**S3-190992 Proposed addition to key issue#1.1 for standalone non-public networks**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190788)

**Decision:** The document was **approved**.

**S3-190789 Adding network binding requirement to the keys issue #1.1 on standalone public networks**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

**Decision:** The document was **revised to S3-190993**.

**S3-190993 Adding network binding requirement to the keys issue #1.1 on standalone public networks**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

(Replaces S3-190789)

**Decision:** The document was **approved**.

**S3-190790 Proposed solution to key issue #1.1 in TR 33.819**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Qualcomm Incorporated*

**Discussion:**

Ericsson: Question whether it was addressing both the requirements proposed in S3-190789. Qualcomm: confirmed this.

**Decision:** The document was **approved**.

**S3-190855 KI on credential storage for NPN-Ues**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **noted**.

**S3-190858 Key issue on secure storage of SNPN access credentials**

 *Type: pCR For: (not specified)
 33.819 v0.2.0
 Source: Samsung, Intel*

**Discussion:**

SA3 agrees to the following: storage of non-3GPP credentials for standalone NPN will not be addressed. This won't stop us from mentioning that they are in the UE.

**Decision:** The document was **noted**.

**S3-190859 Solution for secure storage of SNPN access credentials**

 *Type: pCR For: (not specified)
 33.819 v0.2.0
 Source: Samsung, Intel*

**Decision:** The document was **noted**.

**S3-190860 Key issue on CAG access control in Non-standalone NPNs**

 *Type: pCR For: (not specified)
 33.819 v0.2.0
 Source: Samsung*

**Discussion:**

DCM: Change minimise into mitigate. Ericsson: Checking on the authorisation of the UE to a PLMN. Orange: Title should be aligned with the details of the keys issue.

**Decision:** The document was **revised to S3-190994**.

**S3-190994 Key issue on CAG access control in Non-standalone NPNs**

 *Type: pCR For: -
 33.819 v0.2.0
 Source: Samsung*

(Replaces S3-190860)

**Decision:** The document was **approved**.

**S3-190861 New solution for CAG access control in Non-standalone NPNs**

 *Type: pCR For: (not specified)
 33.819 v0.2.0
 Source: Samsung*

**Discussion:**

Orange: It is FF whether this mechanism protects against DOS attack. Interdigital: Have privacy concerns on the sending the CAG identity. An editor's notes on privacy of CAG was added. Title will be aligned with the change to the key issue.

**Decision:** The document was **revised to S3-190995**.

**S3-190995 New solution for CAG access control in Non-standalone NPNs**

 *Type: pCR For: -
 33.819 v0.2.0
 Source: Samsung*

(Replaces S3-190861)

**Decision:** The document was **approved**.

**S3-190845 Discussion on NPN Authentication**

 *Type: discussion For: Endorsement
 33.819 v..
 Source: Cablelabs, Nokia, Nokia Shanghai Bell*

**Discussion:**

Presented as introduction to the following documents

**Decision:** The document was **noted**.

**S3-190856 KI on authentication and authorization of NPN subscribers by a 5G external entity**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Chair: Is this related to S3-190990 discussion. Orange: Will object to this document whether it is or not. It was questioned who is the 3rd party is in this case. Nokia: It is interface between the AUSF and AAA. Ericsson: Support a re-work of the Key issue to tackle the possible location of the AAA. It was taken offline for further work.

**Decision:** The document was **revised to S3-191000**.

**S3-191000 KI on authentication and authorization of NPN subscribers by a 5G external entity**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-190856)

**Decision:** The document was **approved**.

**S3-190846 Deployment options for authentication in NPNs**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Cablelabs, Nokia, Nokia Shanghai Bell*

**Discussion:**

Orange: Do not want the accept the contribution. Vdf: OK for inclusion. Sony, Huawei & Interdigital support the inclusion. Qualcomm: delete the use of MSK. Gemalto: Want to clarify that these are just example of the possible deployments. Orange: What is the difference between the key issue and the Annex. Ericsson: It is possible to refer to the Annex. Orange: Key Issue will refer to the Annex and also wonders why that is helpful. Idemia: Concern about Key Issue referring to Annex. Ericsson: Include Annex and maybe use some of the content in the Key Issue.

**Decision:** The document was **revised to S3-191001**.

**S3-191001 Deployment options for authentication in NPNs**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Cablelabs, Nokia, Nokia Shanghai Bell*

(Replaces S3-190846)

**Decision:** The document was **approved**.

**S3-190847 Evaluation of EAP-TTLS for non-certificate based UE authentication in SNPNs**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Cablelabs, Nokia, Nokia Shanghai Bell*

**Decision:** The document was **not treated**.

**S3-190848 Solution on non-certificate based UE authentication in 5G NPN with AAA**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Cablelabs, Nokia, Nokia Shanghai Bell*

**Discussion:**

Vdf: Like to see an EN to say "Impact of KH is FFS" as it is not clear whether there is any impact. Orange would like an EN as the KI is not complete. TI: It should be noted as the Key Issue is not complete, Gemalto and Idemia support TI. Ericsson raised concerns about the Phase 2.

**Decision:** The document was **noted**.

**S3-190849 Solution on non-certificate based UE authentication in 5G NPN without AAA**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Cablelabs, Nokia, Nokia Shanghai Bell*

**Discussion:**

Noted due to incomplete KI

**Decision:** The document was **noted**.

**S3-190850 Discussion of security solutions for SNPN service access via PLMN and vice versa**

 *Type: discussion For: Endorsement
 33.819 v..
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **not treated**.

**S3-190851 Solution on SNPN service access via PLMN**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **not treated**.

**S3-190852 Solution on PLMN service access via NPN**

 *Type: pCR For: Approval
 33.819 v16.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **not treated**.

**S3-190853 Discussion on Authentication of UE to PLMN integrated NPN**

 *Type: discussion For: Endorsement
 33.819 v..
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **not treated**.

**S3-190854 Solution for UE authentication to PLMN integrated NPN**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **not treated**.

**S3-190857 Rapporteur correction to TR 33819**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: Nokia, Nokia Shanghai Bell*

**Decision:** The document was **approved**.

**S3-190882 Issue of Alignment of the terms Private network and NPN**

 *Type: pCR For: Approval
 33.819 v0.2.0
 Source: SAMSUNG*

**Decision:** The document was **noted**.

**S3-190990 NPN authentication way forward**

 *Type: discussion For: Endorsement
 Source: ORANGE*

**Discussion:**

Nokia: NPN authentication should be addressed in a new clause in 33.501. Orange: disagree. TI, Gemalto supported Orange proposal. Sony and Samsung support a Nokia proposal. QC suggested adding an extra sentence to say that the existing method could refer to the existing methods. Huawei: NPN operators can chose the authentication method they want. DT: Agree on this but don't want to specify all deals. TI: There are already authentication methods for private networks in TS 33.501. Samsung: raised some concerns on support of methods in NPN.

**Decision:** The document was **revised to S3-190999**.

**S3-191018 draft TR 33.819**

 *Type: draft TR For: Approval
 33.819 v0.3.0
 Source: Nokia*

**Decision:** The document was **approved**.

**S3-190999 NPN authentication way forward**

 *Type: discussion For: Endorsement
 Source: ORANGE*

(Replaces S3-190990)

**Discussion:**

QC: support for algorithm in NPN is not automatically inherited Orange: not for isolated deployments - wordsmithing taken offline. Discussion on modification of SA1 requirement - this wasn't agreed - copy/paste text from Annex B was proposed.

**Decision:** The document was **revised to S3-191003**.

**S3-191003 NPN authentication way forward**

 *Type: discussion For: Endorsement
 Source: ORANGE,Telecom Italia, Huawei*

(Replaces S3-190999)

**Decision:** The document was **endorsed**.

### 5.16 Study on LTKUP Detailed solutions (FS\_LTKUP\_Detail) (Rel-16)

**S3-190768 pCR to 33935 - addition section 4.1 Overview**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: VODAFONE Group Plc*

**Discussion:**

Orange: Modify to SIM/USIM. Gemalto asked to check the solution number. There is a need to modify 2G/3G/4G as these terms not used in specs.

**Decision:** The document was **revised to S3-190953**.

**S3-190953 pCR to 33935 - addition section 4.1 Overview**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: VODAFONE Group Plc*

(Replaces S3-190768)

**Decision:** The document was **approved**.

**S3-190773 pCR to 33935 - addition of detailed solution 4b**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: VODAFONE Group Plc*

**Discussion:**

Orange: Add reference to SIM OTA - remove the two notes. Some changes 4.2.3 that were agreeable. Vdf: UICC should be changed to USIM.

**Decision:** The document was **revised to S3-190954**.

**S3-190954 pCR to 33935 - addition of detailed solution 4b**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: VODAFONE Group Plc*

(Replaces S3-190773)

**Decision:** The document was **approved**.

**S3-190840 Detailed solution 5 in TR 33.935**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: Gemalto N.V.*

**Abstract:**

Addition of detailed solution 5 in 3GPP TR 33.935

**Decision:** The document was **revised to S3-190920**.

**S3-190920 Detailed solution 5 in TR 33.935**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: Gemalto N.V.*

(Replaces S3-190840)

**Discussion:**

Orange had some small changes to document that were agreeable. The reference to eSIM was removed as it about provisioning.

**Decision:** The document was **revised to S3-190955**.

**S3-190955 Detailed solution 5 in TR 33.935**

 *Type: pCR For: Approval
 33.935 v0.0.0
 Source: Gemalto N.V.*

(Replaces S3-190920)

**Decision:** The document was **approved**.

**S3-190956 draft TR 33.935**

 *Type: draft TR For: Approval
 33.935 v0.1.0
 Source: Vodafone*

**Decision:** The document was **approved**.

**S3-191022 Draft skeleton document for TR 33.935**

 *Type: draft TR For: Approval
 33.935 v0.0.0
 Source: Vodafone*

**Discussion:**

Delete the content of the introduction clause

**Decision:** The document was **revised to S3-191024**.

**S3-191024 Draft skeleton document for TR 33.935**

 *Type: draft TR For: Approval
 33.935 v0.0.0
 Source: Vodafone*

(Replaces S3-191022)

**Decision:** The document was **approved**.

### 5.17 Study on User Plane Integrity Protection (FS\_UP\_IP\_Sec) (Rel-16)

**S3-190605 Proposal for FS\_UP\_IP\_Sec Key Issue #1.3: User plane integrity between UE and network**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Philips International B.V.*

**Abstract:**

Proposal for zero overhead user plane integrity protection by using cryptographic CRCs in Transport Blocks and Code Blocks. The error behaviour of the UE-eNodeB link due to noise is unaffected by this integrity protection.

**Discussion:**

Nokia: impact is at physical layer. Not reliable ZTE: PDCP is multiplexed into transport block, how is policy in case of multiplexed being taken care of. Huawei: solution is not within the scope of this TR. Should adopt PDCP from 5G. BT: CRC should be for natural errors, can't distinguish between security and transmission errors. VF: add this solution and then point out all of the problems in evaluation. DT: creative solution, should go in. E//: why is integrity not provided at PDCP layer. Philips: this is zero overhead solution. VF: prefer as two tdocs, with key issue. E//: description of key issue is too global. DCM: not put in key issue. put in solution and then put in evaluation. VF: put in solution and give evaluation. Huawei: this study was understood that it is only about user plane integrity protection at PDCP layer. IDCC: add key issue of overhead QC: support IDCC and Huawei proposal. QC: need agreement that solution should not have impact on physical layer. NEC: note for now. Lot of support for noting it.

**Decision:** The document was **noted**.

**S3-190647 Editorial corrections in TR 33.853 v0.1.0**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd*

**Abstract:**

Editorial changes to TR 33.853.

**Decision:** The document was **approved**.

**S3-190648 Discussion on the need of UP IP solution for Rel.15 UEs**

 *Type: discussion For: Discussion
 33.853 v..
 Source: NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung*

**Abstract:**

This contribution discusses the motivation of a new key issue.

**Decision:** The document was **noted**.

**S3-190649 New key issue on data rate limitation of integrity protection in UP DRB**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung*

**Abstract:**

This contribution introduces a new key issue.

**Discussion:**

Huawei: only support one solution. If operator decides to turn off, then what can one do. VF: not clear that this is serving network decision, so need to be more clear about operators. NEC: if only 64kbit/sec is possible then how can IP be used. Nokia: if IP is turned off, then what can be done? policy needs to be removed. NEC: remove first requirement. how does the user know that there is IP? VF: service level agreement. NEC: support for second part is there. Huawei: when UE doesn't support full data rate, then do something else. E//: what is the key issue we are trying to solve. QC: if no IP protection is enabled, how can the user be protected. VF: if the home operator promises IP, but the serving network doesn't support it, then how could IP be provided. BT: mismatch between the users preference and policy of network. Samsung: differentiate user and protocol perspective VF: whether worth it depends on user expectation. E//: solution targeting R15 UEs, but target solutions that defend if IP is not supported. need to be clarified.

**Decision:** The document was **revised to S3-190911**.

**S3-190911 New key issue on data rate limitation of integrity protection in UP DRB**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung*

(Replaces S3-190649)

**Discussion:**

Modify requirement to refer to security threat clause

**Decision:** The document was **revised to S3-191004**.

**S3-191004 New key issue on data rate limitation of integrity protection in UP DRB**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung*

(Replaces S3-190911)

**Decision:** The document was **approved**.

**S3-190650 New solution for data rate limitation of integrity protection in UP DRB**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd, Lenovo, Motorola Mobility*

**Abstract:**

This contribution introduces a new solution.

**Discussion:**

Ericsson: concerned that it does not address discussed key issue. NEC: aims for Rel-15 UEs. DT: not keen on such solution but if pursued keep as simple as possible and always protect header. Huawei: Maybe a moving window would be better and concern that this needs to be more studied and maybe fooling ourselves that there is integrity protection. QC: think if integrity protection is done, it should be done on full packet. ZTE: Not keen on approach.

**Decision:** The document was **noted**.

**S3-190651 New solution for data rate limitation of integrity protection in UP DRB**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new solution.

**Discussion:**

Ericsson: This a new cryptographic algorithm and we are not doing that in SA3. Huawei: Also concern that this is a new approach to calculating a MAC and needs more justification.

**Decision:** The document was **noted**.

**S3-190652 New key issue on integrity protection capability imbalance in MR-DC scenarios**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new key issue.

**Discussion:**

This was discussed along with S3-190707 and S3-190708. Authors of the various documents agree that it would be possible to merge the docs provided there are requirement for individual options. Huawei: Concern on some of the details of S3-190652. Ericsson think there is no need for the key issue as the issue is whether a ng-eNB supports UP IP. Vdf think that we just need keys issues on the UE being able to support UP IP at full rate. NEC think there are solutions that do not require ng-eNB to support integrity protection. Vdf: The KIs in the current TR are about secure negotiation and activation of the UP IP in EPS. QC proposes that the contributions are merged into one key issue. This work will happen in some offline manner.

**Decision:** The document was **revised to S3-190912**.

**S3-190912 New key issue on integrity protection capability imbalance in MR-DC scenarios**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd*

(Replaces S3-190652)

**Discussion:**

DCM: ng-eNB is already like a solution.

**Decision:** The document was **revised to S3-191019**.

**S3-191019 New key issue on integrity protection capability imbalance in MR-DC scenarios**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd,Huawei*

(Replaces S3-190912)

**Decision:** The document was **approved**.

**S3-190653 New solution for integrity protection capability imbalance in MR-DC scenarios**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: NEC Europe Ltd*

**Abstract:**

This contribution introduces a new solution.

**Discussion:**

Relates to the open key issue resulting from S3-190652. Huawei did not want UP terminating somewhere other than eNB. Vdf propose that the solution is added and the issue are documented. QC raised concern about no IP layer in eNB and non-IP traffic.

**Decision:** The document was **noted**.

**S3-190707 Support UP\_IP in option 7**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

See discussion on S3-190652. Merged into S3-190912.

**Decision:** The document was **merged**.

**S3-190708 UP IP for Option 4**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

See discussion on S3-190652. Merged into S3-190912.

**Decision:** The document was **merged**.

**S3-190802 pCR: New KI: Integrity Algorithm independence**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Qualcomm Incorporated*

(Replaces S3-190388)

**Discussion:**

Vdf wanted clarification that new algorithms should also be considered. DCM: It should only be 4G and 5G algorithms. Orange: Does this apply for optional algorithms as well. QC: Yes as it needs to apply to all algorithms. Ericsson: Does not feel that this key but more of an evaluation criteria. QC: important it applies to all algorithms as UE will report its lowest data rate among all of its supported algorithms.

**Decision:** The document was **revised to S3-190913**.

**S3-190913 pCR: New KI: Integrity Algorithm independence**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Qualcomm Incorporated*

(Replaces S3-190802)

**Discussion:**

On further discussion, other companies had concerns and document is noted.

**Decision:** The document was **noted**.

**S3-190803 pCR: New KI: Ability to prioritize certain PDCP packets on the UE uplink**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Qualcomm Incorporated*

(Replaces S3-190387)

**Discussion:**

Vdf: Would like to qualify that the requirement shall not break the UP IP. This was agreeable. Nokia: Concern about latency. Huawei: Think that this a RAN issue rather than a security issue. Ericsson: Also think that this not a security requirement. DT and Vdf support having a KI on this. Ericsson: Do not believe that this group can look at these layers. Samsung think that this is RAN issue. DCM believe that there is a security issue. Vdf had a proposal to reverse the way the requirement was written.

**Decision:** The document was **revised to S3-190914**.

**S3-190914 pCR: New KI: Ability to prioritize certain PDCP packets on the UE uplink**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Qualcomm Incorporated*

(Replaces S3-190803)

**Decision:** The document was **approved**.

**S3-190804 pCR: New KI: Efficient handling of PDCP discardTimer expiry on the UE Uplink**

 *Type: pCR For: Approval
 33.853 v0.1.0
 Source: Qualcomm Incorporated*

(Replaces S3-190386)

**Discussion:**

Huawei: Do not believe that this a security issue. Ericsson: Agree that this is not a security issue. QC: Issue of re-use of PDCP counter for multiple uses. DT: Believe that there is a security issue and we should start the work in SA3. Intel think that there should be an LS to RAN2 from this meeting. Samsung agree with Intel's proposal. QC are OK to involve in RAN2. Vdf: There is a security issue as there are not full rate UEs. Huawei proposal to merge the key issues in S3-910803 and S3-190804 in one Key Issue that relates to supporting UP IP at full rate. In parallel, there should be an LS to RAN2 to get feedback on the issues that limit the support of full rate UP IP. Apple: Proposal to add key issue details later, but OK to keep requirement. The Key issue details will contains that there was an issue raised by RAN2 and not the specific details.

**Decision:** The document was **merged**.

**S3-190880 (FS\_UP\_IP\_Sec) Integrity protection of the User Plane -New key Issue - Reporting Integrity check failures to the network**

 *Type: discussion For: Decision
 33.853 v..
 Source: BT plc*

**Abstract:**

It is proposed to add a key issue to TR33.853 [3] concerning operation 1) during normal handover between eNB’s and 2) when redundant transmission in the user plane is used to support Ultra Reliable Low Latency Communication URLLC

And add the following

**Discussion:**

Vdf: Editorial formatting is not good. DT: Not sure about this when it was first discussed and it is not clear what the operator would do with the information. QC: do not support the requirement. Samsung: support including this key issue. Huawei: Support the keys issue. Ericsson and Nokia: Don't think that this is in scope of the work of this study item. SA3 think that this a topic that should be studied, but the correct place to study this is FFS.

**Decision:** The document was **noted**.

**S3-190910 draft TR33.853**

 *Type: draft TR For: Approval
 33.853 v0.2.0
 Source: Vodafone*

**Decision:** The document was **approved**.

**S3-190915 LS on Full date rate support for UP IP**

 *Type: LS out For: Approval
 to -
 Source: Qualcomm*

**Discussion:**

DCM: requirements strange wording Huawei: delete supported, remove two bullets.E//: support Huawei DCM: remove bullets, ask RAN2 for technical details for R15 decision. QC: ok, some other rewording. Huawei: remove references in question 1 to above.

Huawei: not include the details that were raised by QC. DCM: request from RAN2 why the limitation was in R15

**Decision:** The document was **revised to S3-191020**.

**S3-191020 LS on Full date rate support for UP IP**

 *Type: LS out For: Approval
 to RAN2, cc RAN, RAN1, RAN3
 Source: Qualcomm*

(Replaces S3-190915)

**Decision:** The document was **approved**.

### 5.18 Study on Security Impacts of Virtualisation (FS\_SIV) (Rel-16)

**S3-190610 Initialisation of Sensitive Functions in a Virtualised Environment**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: ETSI TC CYBER*

**Decision:** The document was **noted**.

### 5.19 Study on authentication enhancements in 5GS (FS\_AUTH\_ENH) (Rel-16)

**S3-190809 Skeleton for TR 33.846**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190810 Scope for TR 33.846**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Ericsson*

**Decision:** The document was **approved**.

**S3-190760 Key issue to ensure the security of session anchor keys**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Decision:** The document was **noted**.

**S3-190690 A key issue on the long-term key and its related anchor key leakage**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Huawei, HiSilicon*

**Decision:** The document was **noted**.

**S3-190811 New KI: Leakage of long-term key**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Ericsson*

**Discussion:**

VF: what is the relation to LTKUP, BT: this is about mitigation, the other is about prevention, seems to be duplicating the response mechanism. E//: unrelated to LTKUP, this is about perfect forward secrecy. E//: solutions also include active attacks, E// only wants to address passive attacks. VF: this was already discussed in several studies. Orange: agree with VF. BT: solution out of this would be to stop a man in the middle. VF: already in solution 4b and 6 out of LTKUP. E//: we had the discussion before. Todor: between agreeing the study item and now, the 9 series TR was discussed. Telenor: assumption of key compromise during production should be out of scope. Orange: this should eventually become a focussed study to update 9 series TR from LTKUP. NEC: agree that assumption of root key compromise is tenacious, but this is about PFS.

**Decision:** The document was **noted**.

**S3-190759 Key issue regarding the minimal computational cost when generating session anchor keys**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

Orange: how was the evaluation done that the current state is not optimal. IDCC: it is not implied that current auth schemes are not effective or efficient. Orange: why is the current authentication from computational perspective not optimal? VF: similar to 256 discussion, difficult to quantify performance, agree with spirit of contribution, but not possible to evaluate against. BT: in IoT space, many and competing performance requirements. Lowest common denominator is only password? NEC: similar to discussion on KDF. Huawei: different, this is on efficiency. IDCC: "may" not fulfil?

**Decision:** The document was **noted**.

**S3-190626 eAUTH-Linkability KI exposure of cause value**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Decision:** The document was **merged**.

**S3-190735 Key issue on linkability attack**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **merged**.

**S3-190762 Key issue to resist the linkability attacks**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

VF: this is only in case of rare auth failures. DCM: fake base station replaying a auth vector. NEC: UE will not camp on cell after two auth failures. Huawei: this allows a DoS. E//: only barred for 5min. ZTE: attacker can change cell ID. VF: should be in FBS study. Huawei: this attack needs to be studied because it is a published attack. VF: support this in this study, but close FBS? E//: referencing the wrong paper. Adrian: needs to be documented here or in FBS. Proposal to merge and then decide to put into FBS or eAUTH TR. NCSC: avoid saying "the linkability attack". E//: leave requirements blank for now.

**Decision:** The document was **revised to S3-190909**.

**S3-190909 Key issue to resist the linkability attacks**

 *Type: pCR For: -
 33.846 v0.0.0
 Source: China Mobile Com. Corporation,ZTE,Huawei*

(Replaces S3-190762)

**Decision:** The document was **approved**.

**S3-190628 eAUTH-Linkability KI SQN exposure**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

QC: keep it open for now, until CR by QC has been decided, then add if not agreed in May meeting. ZTE: this is different key issue. Gemalto: support QC proposal. NEC: also. BT: support, need a list of known attacks. VF: Normal network operator procedures of SQN buckets could be used to prevent this attack. Merge first requirement into 909, second requirement will be reconsidered after the May meeting discussions.

**Decision:** The document was **merged**.

**S3-190627 eAUTH-Linkability KI different length of response**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

QC: the message needs to be protected, not the length. ZTE: even if encrypted, the length will leak which type it is. QC: key issue is assuming that there is a specific solution. IDCC: replace length of response by indistinguishable responses. Orange, VF: support IDCC phrasing NCSC: if this is not about length, then it fits in with 909. Merge to 909

**Decision:** The document was **merged**.

**S3-190621 eAUTH-SUCI KI Computing resource consuming**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

VF: should be "a" privacy mechanism, not "the", can already be done, nothing new required. IDCC: key is not to asymmetric algorithm. VF: are we really worried about DoS attack on computation resource because we have virtual scalable servers. BT: ECC was chosen to avoid performance issues IDCC: right choice, but in case of DDoS attack, there is a problem. support the issue, but not the focus on asymmetric. E//: because UE is limited, and needs to do more work than UDM. TIM: new issue just came up after 6 month - is this to legitimate a new option? NEC: not do this. QC also. DT: also.

**Decision:** The document was **noted**.

**S3-190761 Key issue to mitigate the DDoS attacks on the UDM**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

NCSC: same as previous contribution, same applies? VF: same, or worse, this doesn't even say where the DDoS is coming from.

**Decision:** The document was **noted**.

**S3-190622 eAUTH-SUCI KI congestion**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

VF: in case of proprietary mechanism, UDM is scoped accordingly. BT: this was already agreed with CT, so not an issue. NEC: how can a UE produce false output? E//: already dealt with in 33.501 by rejection of long SUCIs.

**Decision:** The document was **noted**.

**S3-190623 eAUTH-SUCI KI quantum computing**

 *Type: pCR For: Approval
 33.846 v0.3.0
 Source: ZTE Corporation*

**Discussion:**

VF: there is indication which mechanism is being used. NCSC: this will be relevant in 10-20 years time. IDCC: extend to whole scope of authentication, not only SUCI concealment. Orange: quantum study already gave timeline. Juniper: agree. QC: agree. Noted

**Decision:** The document was **noted**.

**S3-190633 New KI on Fast re-authentication procedure for 5GS**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: NEC Europe Ltd, Intel*

**Abstract:**

This pCR proposes a key issue for study item on security for authentication enhancements in 5GS (TR 33.846).

**Discussion:**

ZTE: not covered by scope of SID. NEC: because DoS is in scope, so it should be in scope: QC: not in scope, E//: not in scope, BT: support this contribution. QC: because of horizontal and vertical key handover, auth is rare, currently not a problem. NEC: for as long as staying in the same access, then few authentications, not when changing access. Huawei: with virtualization, you can throw more resources at it. NEC: this is AuC. BT: should be in URLLC work item. ZTE: note it. Normal authentication can be used.

**Decision:** The document was **noted**.

**S3-190813 Update on EAP-AKA´ PFS**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Ericsson*

**Discussion:**

Nokia: what is status of IETF discussion? E//: ongoing email discussion.

**Decision:** The document was **noted**.

**S3-190812 New solution: EAP-AKA´ PFS**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Ericsson*

**Decision:** The document was **noted**.

**S3-190841 33.846: solution for anchor keys security**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Gemalto N.V.*

**Abstract:**

Solution for anchor keys security in 3GPP TR 33.846

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190658 Discussion paper on UE initiated EAP AKA' with PFS**

 *Type: discussion For: Endorsement
 Source: Nokia*

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190659 UE Initiated EAP AKA' PFS solution**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Nokia*

**Abstract:**

This contribution proposes a UE initiated option for EAP AKA with PFS

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190691 Solution Proposal based on DH between UE and AUSF**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Huawei, HiSilicon*

**Discussion:**

NCSC: no DH for SUPI protection, but ECDH. No key issue, noted

**Decision:** The document was **noted**.

**S3-190763 Security enhancement for the key KSEAF based on the symmetric algorithm**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

VF: long term key can be updated anyways in IoT. No key issue

**Decision:** The document was **noted**.

**S3-190764 KSEAF enhancement for the EAP-AKA’ protocol**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

VF: same as before

**Decision:** The document was **noted**.

**S3-190839 New solution: Deriving session anchor keys with random number**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation, Nubia*

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190765 ECIES based security enhancement for the key KSEAF**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190766 KSEAF enhancement for 5G AKA protocol**

 *Type: pCR For: (not specified)
 33.846 v0.0.0
 Source: China Mobile Com. Corporation*

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190629 eAUTH-Linkability solution encrypted session anchor key based solution**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

related to 909 discussion E//: related to linkability, VF: is this backwards compatible ZTE: yes - closed temporarily until requirement was approved. QC: step 7 - how does the AMF verify the response. ZTE: Provide a response. NEC: Using keys for an authentication is a fundamental change. QC: this is no longer AKA. Nokia: Man in the middle attack seems to be still possible.

**Decision:** The document was **noted**.

**S3-190736 New solution for linkability attack**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

related to 90 discussion. QC: how does it work for NULL scheme. DCM: if no SUPI privacy, then the UE gives SUPI. Ericsson: Only seems to work for initial authentication - add an EN/text to show its works for re-authentication. QC: add EN on how this works with a Rel-15 USIM. Orange: SIDF has the private key and is the entity that can decrypt the response. NEC: Add an EN on Impacts on UDM is FFS. QC: Unclear how the UDM know which UE is failing its authentication. Huawei: Needs some keep alive. Nokia: The solution need more expansion as there are so many questions.

**Decision:** The document was **noted**.

**S3-190625 eAUTH-SUCI solution mitigation of large SUCI attack**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190624 eAUTH-SUCI solution adding symmetric algorithm for SUPI protection scheme**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

no key issue for this VF: secret key shall not leave the USIM, otherwise makes no sense. Exactly as specified in 33.501. secret key shared across a batch of USIMs.

**Decision:** The document was **noted**.

**S3-190634 Solution to support Fast Re-authentication in 5GS**

 *Type: pCR For: Approval
 33.846 v0.0.0
 Source: NEC Europe Ltd, Intel*

**Abstract:**

This pCR proposes a solution to support fast re-authentication to study item on authentication enhancements in 5GS (TR 33.846).

**Discussion:**

no key issue for this

**Decision:** The document was **noted**.

**S3-190908 Draft TR 33.846**

 *Type: draft TR For: Approval
 33.846 v0.1.0
 Source: Ericsson*

**Decision:** The document was **approved**.

### 5.20 Study on Security for NR Integrated Access and Backhaul (FS\_NR\_IAB\_Sec)

**S3-190863 Draft TR 33.xxx - Skeleton TR on Security for NR Integrated Access and Backhaul**

 *Type: other For: (not specified)
 Source: Samsung*

**Decision:** The document was **approved**.

**S3-190864 Scope for the study on security for NR Integrated Access and Backhaul**

 *Type: other For: (not specified)
 Source: Samsung*

**Decision:** The document was **revised to S3-190916**.

**S3-190916 Scope for the study on security for NR Integrated Access and Backhaul**

 *Type: other For: -
 Source: Samsung*

(Replaces S3-190864)

**Decision:** The document was **approved**.

**S3-190917 new draft TR 33.XYZ**

 *Type: other For: Approval
 Source: Samsung*

**Decision:** The document was **approved**.

### 5.21 Study on Security Aspects of 3GPP support for Advanced V2X Services (FS\_eV2X\_Sec)

**S3-190601 New Key Issue for eV2X TR - privacy protection for unicast messages**

 *Type: other For: Approval
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes a new KI for eV2X TR.

**Decision:** The document was **noted**.

**S3-190602 New Key Issue for eV2X TR - privacy protection for multicast messages**

 *Type: other For: Approval
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes a new KI for eV2X TR.

**Decision:** The document was **noted**.

**S3-190604 New Key Issue for eV2X TR - security for unicast/multicast messages**

 *Type: other For: Approval
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes a new KI for eV2X TR.

**Decision:** The document was **noted**.

**S3-190606 New Key Issue for eV2X TR - Security of the UE service authorization and revocation**

 *Type: other For: Approval
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes a new KI for eV2X TR.

**Decision:** The document was **noted**.

**S3-190607 New Key Issue for eV2X TR - Security of the UE service provisioning**

 *Type: other For: Approval
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes a new KI for eV2X TR.

**Decision:** The document was **noted**.

**S3-190608 References**

 *Type: other For: Approval
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes References Section for eV2X TR.

**Decision:** The document was **noted**.

**S3-190769 Skeleton of eV2X security study**

 *Type: other For: Approval
 Source: LG Electronics*

**Decision:** The document was **approved**.

**S3-190770 Scope proposal for eV2X security study**

 *Type: other For: Approval
 Source: LG Electronics*

**Discussion:**

3 small changes to align with drafting rules

**Decision:** The document was **revised to S3-190918**.

**S3-190918 Scope proposal for eV2X security study**

 *Type: other For: Approval
 Source: LG Electronics*

(Replaces S3-190770)

**Decision:** The document was **approved**.

**S3-190919 new draft TR 33.ABC**

 *Type: other For: Approval
 Source: LG*

**Decision:** The document was **approved**.

## 6 Any Other Business

**S3-190612 Work Plan input from Rapporteurs**

 *Type: other For: (not specified)
 Source: WG Vice Chairs*

**Decision:** The document was **revised to S3-191035**.

**S3-191035 Work Plan input from Rapporteurs**

 *Type: other For: -
 Source: WG Vice Chairs*

(Replaces S3-190612)

**Decision:** The document was **noted**.

## Annex A: List of contribution documents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document | Title | Source | Decision | Replaces | Replaced by |
| S3-190600 | Agenda | WG Vice Chair | revised |  | S3-190921 |
| S3-190601 | New Key Issue for eV2X TR - privacy protection for unicast messages | InterDigital, Inc. | noted |  |  |
| S3-190602 | New Key Issue for eV2X TR - privacy protection for multicast messages | InterDigital, Inc. | noted |  |  |
| S3-190603 | Solution proposal for FS\_CIoT\_sec\_5G key issue #1 and #2 | Philips International B.V. | revised |  | S3-191027 |
| S3-190604 | New Key Issue for eV2X TR - security for unicast/multicast messages | InterDigital, Inc. | noted |  |  |
| S3-190605 | Proposal for FS\_UP\_IP\_Sec Key Issue #1.3: User plane integrity between UE and network | Philips International B.V. | noted |  |  |
| S3-190606 | New Key Issue for eV2X TR - Security of the UE service authorization and revocation | InterDigital, Inc. | noted |  |  |
| S3-190607 | New Key Issue for eV2X TR - Security of the UE service provisioning | InterDigital, Inc. | noted |  |  |
| S3-190608 | References | InterDigital, Inc. | noted |  |  |
| S3-190609 | Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN | InterDigital, Inc. | revised |  | S3-191002 |
| S3-190610 | Initialisation of Sensitive Functions in a Virtualised Environment | ETSI TC CYBER | noted |  |  |
| S3-190611 | Reply LS on authentication of group of IoT devices | S1-190501 | postponed |  |  |
| S3-190612 | Work Plan input from Rapporteurs | WG Vice Chairs | revised |  | S3-191035 |
| S3-190613 | New Solution: Battery efficient AKMA | KPN N.V. | revised |  | S3-190926 |
| S3-190614 | Update of Solution #6 – Use of UE Configuration Update | KPN N.V. | noted |  |  |
| S3-190615 | False base station key issue for RLOS P-CR | SPRINT Corporation | noted |  |  |
| S3-190616 | Reduced confidentiality protection key issue for RLOS P-CR | SPRINT Corporation | noted |  |  |
| S3-190617 | Fraud controls bypassed key issue for RLOS P-CR | SPRINT Corporation | noted |  |  |
| S3-190618 | SCAS NEF Add test steps for authorization on northbound APIs | ZTE Corporation | revised |  | S3-190894 |
| S3-190619 | URLLC-KI UP security performance for low latency | ZTE Corporation | revised |  | S3-190969 |
| S3-190620 | URLLC-solution Enhancement of handover with Xn forwarding tunnel | ZTE Corporation | noted |  |  |
| S3-190621 | eAUTH-SUCI KI Computing resource consuming | ZTE Corporation | noted |  |  |
| S3-190622 | eAUTH-SUCI KI congestion | ZTE Corporation | noted |  |  |
| S3-190623 | eAUTH-SUCI KI quantum computing | ZTE Corporation | noted |  |  |
| S3-190624 | eAUTH-SUCI solution adding symmetric algorithm for SUPI protection scheme | ZTE Corporation | noted |  |  |
| S3-190625 | eAUTH-SUCI solution mitigation of large SUCI attack | ZTE Corporation | noted |  |  |
| S3-190626 | eAUTH-Linkability KI exposure of cause value | ZTE Corporation | merged |  | S3-190909 |
| S3-190627 | eAUTH-Linkability KI different length of response | ZTE Corporation | merged |  | S3-190909 |
| S3-190628 | eAUTH-Linkability KI SQN exposure | ZTE Corporation | merged |  | S3-190909 |
| S3-190629 | eAUTH-Linkability solution encrypted session anchor key based solution | ZTE Corporation | noted |  |  |
| S3-190630 | 5GFBS-solution Using symmetric algorithm with assistance of USIM and home network | ZTE Corporation | noted | S3-190155 |  |
| S3-190631 | Evaluation and text for resolving editor’s note for solution #5 in TR 33.825 | NEC Europe Ltd | merged |  | S3-190971 |
| S3-190632 | Solution to KI#9 Key separation for AKMA AFs | NEC Europe Ltd | revised |  | S3-190927 |
| S3-190633 | New KI on Fast re-authentication procedure for 5GS | NEC Europe Ltd, Intel | noted |  |  |
| S3-190634 | Solution to support Fast Re-authentication in 5GS | NEC Europe Ltd, Intel | noted |  |  |
| S3-190635 | Updating Key issue #3 for Network detection of nearby false base station | NEC Europe Ltd | revised |  | S3-190944 |
| S3-190636 | Solution for preventing UE camping on false base station during Idle mode | NEC Europe Ltd | withdrawn |  |  |
| S3-190637 | New Test Case: Error handling of malformed N32 signalling message sent between peer SEPPs | NEC Europe Ltd | noted |  |  |
| S3-190638 | New Test Case: Error handling of malformed JSON object between two network products  | NEC Europe Ltd | noted |  |  |
| S3-190639 | Solution for Established Key Synchronization | NEC Europe Ltd | revised |  | S3-190929 |
| S3-190640 | Discussion on use of established keys for AKMA root key | NEC Europe Ltd | noted |  |  |
| S3-190641 | Discussion on using KSEAF and/or KAUSF for AKMA in view of regulatory compliance  | NEC Europe Ltd | noted |  |  |
| S3-190642 | Resolving Editor’s Notes in Solution #16 | NEC Europe Ltd | approved |  |  |
| S3-190643 | Solution for Roaming Architecture  | NEC Europe Ltd | noted |  |  |
| S3-190644 | Updating solution #16 to include home network option  | NEC Europe Ltd | revised |  | S3-190930 |
| S3-190645 | Creating a combined solution for usage of KSEAF and KAUSF  | NEC Europe Ltd | revised |  | S3-190996 |
| S3-190646 | New KI on Synchronization of Keys when using established keys | NEC Europe Ltd | approved |  |  |
| S3-190647 | Editorial corrections in TR 33.853 v0.1.0 | NEC Europe Ltd | approved |  |  |
| S3-190648 | Discussion on the need of UP IP solution for Rel.15 UEs | NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung | noted |  |  |
| S3-190649 | New key issue on data rate limitation of integrity protection in UP DRB | NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung | revised |  | S3-190911 |
| S3-190650 | New solution for data rate limitation of integrity protection in UP DRB | NEC Europe Ltd, Lenovo, Motorola Mobility | noted |  |  |
| S3-190651 | New solution for data rate limitation of integrity protection in UP DRB | NEC Europe Ltd | noted |  |  |
| S3-190652 | New key issue on integrity protection capability imbalance in MR-DC scenarios | NEC Europe Ltd | revised |  | S3-190912 |
| S3-190653 | New solution for integrity protection capability imbalance in MR-DC scenarios | NEC Europe Ltd | noted |  |  |
| S3-190654 | Notifying cell information to the network after authentication procedure failure | NEC Europe Ltd | revised |  | S3-190998 |
| S3-190655 | Protection of UE configuration against false base station | NEC Europe Ltd | noted |  |  |
| S3-190656 | NSSAI protection during the RRC connection establishment procedure | NEC Europe Ltd | noted |  |  |
| S3-190657 | NSSAI protection during the RRC connection establishment procedure | NEC Europe Ltd | noted |  |  |
| S3-190658 | Discussion paper on UE initiated EAP AKA' with PFS | Nokia | noted |  |  |
| S3-190659 | UE Initiated EAP AKA' PFS solution | Nokia | noted |  |  |
| S3-190660 | Network detection of false base station from UE measurement reports | Nokia | revised |  | S3-190946 |
| S3-190661 | Deleting EN on the usage of per-gNB and per-UE counters for solution #7 “protecting gNB from RRC DoS attack” | Huawei, Hisilicon | revised |  | S3-191025 |
| S3-190662 | Delete the EN related to the “AttackInformationNotification” message | Huawei, Hisilicon | approved |  |  |
| S3-190663 | Propose a new KI and security requirement for spoofing paging messages | Huawei, Hisilicon | noted |  |  |
| S3-190664 | Protection for Incoming Paging Message Based on Stored Security Context | Huawei, Hisilicon | noted |  |  |
| S3-190665 | Avoiding UE connecting to fake base station during HO | Huawei, Hisilicon | revised |  | S3-190947 |
| S3-190666 | Measurement report requirement for the case when the UE in RRC-IDLE & RRC-INACTIVE | Huawei, Hisilicon | merged |  | S3-190985 |
| S3-190667 | Protection of RRSResumeCause | Huawei, Hisilicon | noted |  |  |
| S3-190668 | RRCResume replay protection | Huawei, Hisilicon | noted |  |  |
| S3-190669 | New security requirement against tampering of RRCResumeRequest message | Huawei, Hisilicon | revised |  | S3-190936 |
| S3-190670 | New security requirement against replay of RRCResumeRequest message | Huawei, Hisilicon | revised |  | S3-190937 |
| S3-190671 | Measurement Report Requirement When UE in RRC-CONNECTED | Huawei, Hisilicon | merged |  | S3-190985 |
| S3-190672 | Living Document: General SBA/SBI aspects in TS 33.117 | Nokia, Nokia Shanghai Bell | revised |  | S3-190897 |
| S3-190673 | Handling of UE configuration update by a fake base station | NEC Europe Ltd | withdrawn |  |  |
| S3-190674 | Notifying cell information to the network when the UE determines that the network fails the authentication procedure | NEC Europe Ltd | withdrawn |  |  |
| S3-190675 | Key Issue for Fake Base Station | Intel Mobile Communications | noted |  |  |
| S3-190676 | Cell Authenticated Access for fake base station detection | Intel Mobile Communications | noted |  |  |
| S3-190677 | conclusion for key issue 3 | Huawei, HiSilicon | noted |  |  |
| S3-190678 | conclusion for key issue 6 | Huawei, HiSilicon | approved |  |  |
| S3-190679 | solution 2 clarification | Huawei, HiSilicon | revised |  | S3-190977 |
| S3-190680 | deleting the EN of solution3 | Huawei, HiSilicon | revised |  | S3-190975 |
| S3-190681 | overall introduction | Huawei, HiSilicon | approved |  |  |
| S3-190682 | URLLC solution5 update | Huawei, HiSilicon | revised |  | S3-190971 |
| S3-190683 | evaluation of solution 3 | Huawei, HiSilicon | revised |  | S3-190976 |
| S3-190684 | conclusion for key issue 4 | Huawei, HiSilicon | noted |  |  |
| S3-190685 | solution1 and evaluation update | Huawei, HiSilicon | revised |  | S3-190974 |
| S3-190686 | conclusion for key issue 1 | Huawei, HiSilicon | noted |  |  |
| S3-190687 | conclusion for key issue 2 | Huawei, HiSilicon | noted |  |  |
| S3-190688 | improvement for AKMA architecture | Huawei, HiSilicon | noted |  |  |
| S3-190689 | Dynamic UP security policy control solution for URLLC | Huawei, HiSilicon | revised |  | S3-190972 |
| S3-190690 | A key issue on the long-term key and its related anchor key leakage | Huawei, HiSilicon | noted |  |  |
| S3-190691 | Solution Proposal based on DH between UE and AUSF | Huawei, HiSilicon | noted |  |  |
| S3-190692 | Discussions on solutions to AMF key separation | Huawei, HiSilicon | noted |  |  |
| S3-190693 | AMF key separation solution 1 | Huawei, HiSilicon | noted |  |  |
| S3-190694 | AMF key separation solution 2 | Huawei, HiSilicon | noted |  |  |
| S3-190695 | AMF key separation solution 3 | Huawei, HiSilicon | noted |  |  |
| S3-190696 | Discussion on provisioning security features for a network slice | Huawei, HiSilicon | noted |  |  |
| S3-190697 | Amendment to solution #2 | Huawei, HiSilicon | noted |  |  |
| S3-190698 | Amendment to solution #3 | Huawei, HiSilicon | revised |  | S3-191007 |
| S3-190699 | Amendment to KI#6 | Huawei, HiSilicon | noted |  |  |
| S3-190700 | Discussion on NPN authentication | Huawei, HiSilicon | revised |  | S3-190962 |
| S3-190701 | Evaluation of solution 4 | Huawei, Hisilicon | noted |  |  |
| S3-190702 | Key issue on Key freshness in AKMA | Huawei, Hisilicon | revised |  | S3-190924 |
| S3-190703 | Solution for Key freshness in AKMA | Huawei, Hisilicon | revised |  | S3-191005 |
| S3-190704 | Solution to identify misbehaving UEs | Huawei, Hisilicon | revised |  | S3-191028 |
| S3-190705 | Solution to Migitate DDoS Attack based on RAN | Huawei, Hisilicon | revised |  | S3-191029 |
| S3-190706 | Conclusion for KDF negotiation for 5G System Security | Huawei, Hisilicon | revised |  | S3-190723 |
| S3-190707 | Support UP\_IP in option 7 | Huawei, Hisilicon | merged |  | S3-191019 |
| S3-190708 | UP IP for Option 4 | Huawei, Hisilicon | merged |  | S3-191019 |
| S3-190709 | Add content to section 4 | Huawei, Hisilicon | noted |  |  |
| S3-190710 | Add content to Introduction clause | Huawei, Hisilicon | noted |  |  |
| S3-190711 | Add content to section 4 | Huawei, Hisilicon | withdrawn |  |  |
| S3-190712 | Conclusion on KI#1 | Huawei, Hisilicon | withdrawn |  |  |
| S3-190713 | Delete EN for solution #3 | Huawei, Hisilicon | noted |  |  |
| S3-190714 | Add evaluation to solution #3 | Huawei, Hisilicon | noted |  |  |
| S3-190715 | Delete EN for solution 5 | Huawei, Hisilicon | withdrawn |  |  |
| S3-190716 | Add evaluation to soluiton 5 | Huawei, Hisilicon | withdrawn |  |  |
| S3-190717 | Update to solution#12"DDoS attack mitigation in CIoT" | Huawei, Hisilicon | approved |  |  |
| S3-190718 | Solution for updating key to broadcast assitance data | Huawei, Hisilicon | noted |  |  |
| S3-190719 | Key Issue for encryption and integrity protection of assistance data | Huawei, Hisilicon | noted |  |  |
| S3-190720 | Key Issue for encryption and integrity protection of location data | Huawei, Hisilicon | merged |  | S3-190900 |
| S3-190721 | Key Issue for privacy setting integrity between UE and homenetwork | Huawei, Hisilicon | noted |  |  |
| S3-190722 | Solution on integrity protection of privacy setting between UE and UDM | Huawei, Hisilicon | noted |  |  |
| S3-190723 | Conclusion for KDF negotiation for 5G System Security | Huawei, Hisilicon | revised | S3-190706 | S3-190957 |
| S3-190724 | Draft LS on SCP security requirements | Deutsche Telekom AG | merged |  | S3-190963 |
| S3-190725 | Key Issue: Handling of invalid IPX patches | Deutsche Telekom AG | revised |  | S3-190984 |
| S3-190726 | Key Issue: Protection of SCP interfaces | Deutsche Telekom AG | merged |  | S3-190967 |
| S3-190727 | Key Issue: Secure message transport via the SCP | Deutsche Telekom AG | revised |  | S3-190968 |
| S3-190728 | Test Case: Connection-specific scope of IPX-provider cryptographic material | Deutsche Telekom AG | revised |  | S3-190891 |
| S3-190729 | pCR to TR33.814 - Key issue for positioning data confidentiality protection | CATT | revised |  | S3-190900 |
| S3-190730 | pCR to TR33.814 - Solution for positioning data confidentiality protection | CATT | noted |  |  |
| S3-190731 | pCR to TR33.814 – Text for Clause Introduction | CATT | revised |  | S3-190898 |
| S3-190732 | Text for Clause 4 Security aspects of eLCS | CATT | revised |  | S3-190899 |
| S3-190733 | New requirment for Authentication relay attack | Huawei, Hisilicon | revised |  | S3-190986 |
| S3-190734 | New solution for Authentication relay attack | Huawei, Hisilicon | revised |  | S3-190987 |
| S3-190735 | Key issue on linkability attack | Huawei, Hisilicon | merged |  | S3-190909 |
| S3-190736 | New solution for linkability attack | Huawei, Hisilicon | noted |  |  |
| S3-190737 | New KI: flexible protection of data exchange on N9 | Huawei, Hisilicon | revised |  | S3-190965 |
| S3-190738 | Remove EN in 6.6.3 | Huawei, Hisilicon | revised |  | S3-191008 |
| S3-190739 | Solution for slice specific authorization | Huawei, Hisilicon | revised |  | S3-191009 |
| S3-190740 | SCAS: AMF-specific adaptations of security functional requirements and related test cases | Huawei, Hisilicon | revised |  | S3-190884 |
| S3-190741 | Security Assurance Requirements and Test Case for UPF | Huawei, Hisilicon | revised |  | S3-190885 |
| S3-190742 | Security Assurance Requirement and Test for NRF | Huawei, Hisilicon | revised |  | S3-190978 |
| S3-190743 | Security Assurance Requirement and test cases for SMF | Huawei, Hisilicon | revised |  | S3-190889 |
| S3-190744 | New Key Issue: Support of a UP gateway function on the N9 interface | Ericsson | revised |  | S3-190964 |
| S3-190745 | New KI: N3GPP Key Hierarchy | Ericsson | revised |  | S3-191012 |
| S3-190746 | New Solution: New access type distinguisher for N3GPP | Ericsson | noted |  |  |
| S3-190747 | New Solution: Key separation for untrusted and trusted access | Ericsson | revised |  | S3-191030 |
| S3-190748 | New Solution: SUCI deconcealment for the FN-RG | Ericsson | noted |  |  |
| S3-190749 | The purpose and scope of SCAS | Ericsson | revised |  | S3-190883 |
| S3-190750 | New KI: Interworking between AKMA and GBA | Ericsson | noted |  | - |
| S3-190751 | New solution: WLAN measurements from UEs | Ericsson | revised |  | S3-190905 |
| S3-190752 | New solution: Bluetooth measurements from UEs | Ericsson | revised |  | S3-190906 |
| S3-190753 | Update KI: TBS positioning | Ericsson | approved |  |  |
| S3-190754 | New solution: TBS measurements from UEs | Ericsson | revised |  | S3-190907 |
| S3-190755 | New KI: Privacy control in LCS | Ericsson | revised |  | S3-190902 |
| S3-190756 | New solution: Effective privacy control in LCS | Ericsson | revised |  | S3-190904 |
| S3-190757 | Considerations on network product class when using NFV technology | China Mobile Com. Corporation | revised |  | S3-190951 |
| S3-190758 | Considerations on SECAM of the virtualized network products | China Mobile Com. Corporation | revised |  | S3-190952 |
| S3-190759 | Key issue regarding the minimal computational cost when generating session anchor keys | China Mobile Com. Corporation | noted |  |  |
| S3-190760 | Key issue to ensure the security of session anchor keys | China Mobile Com. Corporation | noted |  |  |
| S3-190761 | Key issue to mitigate the DDoS attacks on the UDM | China Mobile Com. Corporation | noted |  |  |
| S3-190762 | Key issue to resist the linkability attacks | China Mobile Com. Corporation | revised |  | S3-190909 |
| S3-190763 | Security enhancement for the key KSEAF based on the symmetric algorithm  | China Mobile Com. Corporation | noted |  |  |
| S3-190764 | KSEAF enhancement for the EAP-AKA’ protocol | China Mobile Com. Corporation | noted |  |  |
| S3-190765 | ECIES based security enhancement for the key KSEAF | China Mobile Com. Corporation | noted |  |  |
| S3-190766 |  KSEAF enhancement for 5G AKA protocol | China Mobile Com. Corporation | noted |  |  |
| S3-190767 | AKMA Architecture and procedures with the anchor function as NEF | China Mobile Com. Corporation | noted |  |  |
| S3-190768 | pCR to 33935 - addition section 4.1 Overview | VODAFONE Group Plc | revised |  | S3-190953 |
| S3-190769 | Skeleton of eV2X security study | LG Electronics | approved |  |  |
| S3-190770 | Scope proposal for eV2X security study | LG Electronics | revised |  | S3-190918 |
| S3-190771 | Key issue on Granularity of isolation for slice specific security | LG Electronics | noted |  |  |
| S3-190772 | Key issue on UE location privacy setting | LG Electronics | noted |  |  |
| S3-190773 | pCR to 33935 - addition of detailed solution 4b | VODAFONE Group Plc | revised |  | S3-190954 |
| S3-190774 | Resolving Editor's notes in solution 6 | China Mobile Com. Corporation | revised |  | S3-190931 |
| S3-190775 | SCAS 5G: mutual authentication between NFs | Nokia, Nokia Shanghai Bell | revised |  | S3-190896 |
| S3-190776 | Certificate based solution against false base station | Apple Computer Trading Co. Ltd | noted |  |  |
| S3-190777 | SCAS 5G: update to Access Token Verification Failure in non-roaming case | Nokia, Nokia Shanghai Bell | approved |  |  |
| S3-190778 | SCAS 5G: update to Access Token Verification Failure in roaming case | Nokia, Nokia Shanghai Bell | approved |  |  |
| S3-190779 | SCAS 5G: Search Result Handling for NF Discovery | Nokia, Nokia Shanghai Bell | noted |  |  |
| S3-190780 | SCAS SEPP: Serving PLMN ID Mismatch | Nokia, Nokia Shanghai Bell | revised |  | S3-190892 |
| S3-190781 | Proposed evaluation for Solution #1 AS and NAS security for RLOS services | Qualcomm Incorporated | revised |  | S3-191010 |
| S3-190782 | Proposed evaluation for Solution #2 AS and NAS security based on the emergency call procedures | Qualcomm Incorporated | noted |  |  |
| S3-190783 | Proposed update for Solution #2 AS and NAS security based on the emergency call procedures | Qualcomm Incorporated | revised |  | S3-191011 |
| S3-190784 | Acknowledging the multiple possible mobility solutions for CP small data | Qualcomm Incorporated | approved |  |  |
| S3-190785 | Resolving the editor’s note in solution #10 in TR 33.861 | Qualcomm Incorporated | approved |  |  |
| S3-190786 | Adding an evaluation to solution #10 in TR 33.861 | Qualcomm Incorporated | revised |  | S3-191033 |
| S3-190787 | Proposed solution to the key hierarchy for non-public networks | Qualcomm Incorporated | revised |  | S3-190991 |
| S3-190788 | Proposed addition to key issue#1.1 for standalone non-public networks | Qualcomm Incorporated | revised |  | S3-190992 |
| S3-190789 | Adding network binding requirement to the keys issue #1.1 on standalone public networks | Qualcomm Incorporated | revised |  | S3-190993 |
| S3-190790 | Proposed solution to key issue #1.1 in TR 33.819 | Qualcomm Incorporated | approved |  |  |
| S3-190791 | Proposed solution for protecting the S-NSSAI for transmission at the AS layer | Qualcomm Incorporated | noted |  |  |
| S3-190792 | Security protection of small data at idle mode mobility | Qualcomm Incorporated | approved |  |  |
| S3-190793 | Protection against Man-in-the-Middle false base station attacks | Qualcomm Incorporated | revised | S3-190381 | S3-190988 |
| S3-190794 | Conclusion on KI #3 for Study on the security for URLLC | Qualcomm Incorporated | noted |  |  |
| S3-190795 | Conclusion on KI #4 for Study on the security for URLLC | Qualcomm Incorporated | noted |  |  |
| S3-190796 | Conclusion on KI #6 for Study on the security for URLLC | Qualcomm Incorporated | noted |  |  |
| S3-190797 | Conclusion on KI #8 for Study on the security for URLLC | Qualcomm Incorporated | approved |  |  |
| S3-190798 | Changing the security requirement for KI #2 | Qualcomm Incorporated | revised |  | S3-190940 |
| S3-190799 | KAMF separation using a standalone SEAF | Qualcomm Incorporated | noted |  |  |
| S3-190800 | Adding an evaluation to solution #9 in TR 33.861 | Qualcomm Incorporated | revised |  | S3-191032 |
| S3-190801 | pCR: Reusing KAUSF for AKMA | Qualcomm Incorporated | revised | S3-190385 | S3-190928 |
| S3-190802 | pCR: New KI: Integrity Algorithm independence | Qualcomm Incorporated | revised | S3-190388 | S3-190913 |
| S3-190803 | pCR: New KI: Ability to prioritize certain PDCP packets on the UE uplink | Qualcomm Incorporated | revised | S3-190387 | S3-190914 |
| S3-190804 | pCR: New KI: Efficient handling of PDCP discardTimer expiry on the UE Uplink | Qualcomm Incorporated | merged | S3-190386 | S3-190914 |
| S3-190805 | SCAS NRF: Scope Representation for Nnrf\_AccessToken Service | Nokia, Nokia Shanghai Bell | noted |  |  |
| S3-190806 | Evaluation of solution 2 | Ericsson | noted |  |  |
| S3-190807 | Protocol details for solution 3 | Ericsson | approved |  |  |
| S3-190808 | Evaluation of solution 3 | Ericsson | noted |  |  |
| S3-190809 | Skeleton for TR 33.846 | Ericsson | approved |  |  |
| S3-190810 | Scope for TR 33.846 | Ericsson | approved |  |  |
| S3-190811 | New KI: Leakage of long-term key | Ericsson | noted |  |  |
| S3-190812 | New solution: EAP-AKA´ PFS | Ericsson | noted |  |  |
| S3-190813 | Update on EAP-AKA´ PFS | Ericsson | noted |  |  |
| S3-190814 | Solution for key separation based on slice authentication keys | Ericsson | noted |  |  |
| S3-190815 | Evaluation to Solution #3 ‘Security solution for MO SMS at AMF re-allocation’ | Ericsson | approved |  |  |
| S3-190816 | Evaluation to Solution #4 ‘Security solution for UL small data transfer in RRC Suspend and Resume with early data transmission (EDT)’ | Ericsson | noted |  |  |
| S3-190817 | Evaluation to Solution #5 ‘Security solution for small data included in initial NAS signalling at mobility’ | Ericsson | approved |  |  |
| S3-190818 | Solution #Y: Security for redundant data transmission using Dual Connectivity | Ericsson | revised |  | S3-190973 |
| S3-190819 | New solution for security for redundant data transmission using Dual Connectivity procedures | Ericsson | revised |  | S3-190970 |
| S3-190820 | Correction to solution #3 ‘Security policy handling for redundant data transmission’ | Ericsson | approved |  |  |
| S3-190821 | Updates to Solution #14 | Ericsson | noted |  |  |
| S3-190822 | Conclusion to Solution #14 | Ericsson | noted |  |  |
| S3-190823 | New Solution Key Lifetime | Ericsson | noted |  |  |
| S3-190824 | Updates to KI #14 | Ericsson | revised |  | S3-190925 |
| S3-190825 | KI#3 in TR 33.809 - updates to updates to details and threats | Ericsson | approved |  |  |
| S3-190826 | KI#3 in TR 33.809 - updates to requirements | Ericsson | revised |  | S3-190945 |
| S3-190827 | KI#3 in TR 33.809 - new solution for enriched measurement reports | Ericsson | revised |  | S3-190985 |
| S3-190828 | KI#3 in TR 33.809 - conclusion on second requirement (reactive action) | Ericsson | noted |  |  |
| S3-190829 | KI#1 in TR 33.809 - new solution with netwrok controlled RRC Reject message | Ericsson | noted |  |  |
| S3-190830 | New annex in TR 33.809 - summary of PWS security study | Ericsson | noted |  |  |
| S3-190831 | KI#2 in TR 33.809 – updated details (cleanup) | Ericsson | revised |  | S3-190939 |
| S3-190832 | KI#2 in TR 33.809 – new solution for tamper resistant SI messages | Ericsson | revised |  | S3-190941 |
| S3-190833 | ID based solution against false base station | Apple Computer Trading Co. Ltd | noted |  |  |
| S3-190834 | Adding evaluation for Solution #1 | Apple Computer Trading Co. Ltd | revised |  | S3-190938 |
| S3-190835 | Adding evaluation for Solution #2  | Apple Computer Trading Co. Ltd | revised |  | S3-190942 |
| S3-190836 | Modification of user identity in solution 2 and solution 3 | ZTE Corporation, Nubia | noted |  |  |
| S3-190837 | Improvement to key issue #5 | ZTE Corporation, Nubia | noted |  |  |
| S3-190838 | Detection of false relay base station by UE | ZTE Corporation, Nubia | noted |  |  |
| S3-190839 | New solution: Deriving session anchor keys with random number | ZTE Corporation, Nubia | noted |  |  |
| S3-190840 | Detailed solution 5 in TR 33.935 | Gemalto N.V. | revised |  | S3-190920 |
| S3-190841 | 33.846: solution for anchor keys security | Gemalto N.V. | noted |  |  |
| S3-190842 | Solution 15 editorials | Ericsson | revised |  | S3-190932 |
| S3-190843 | Solution 15 comment on the application keys | Ericsson | revised |  | S3-190933 |
| S3-190844 | Solution 15 evaluation | Ericsson | revised |  | S3-190935 |
| S3-190845 | Discussion on NPN Authentication | Cablelabs, Nokia, Nokia Shanghai Bell | noted |  |  |
| S3-190846 | Deployment options for authentication in NPNs | Cablelabs, Nokia, Nokia Shanghai Bell | revised |  | S3-191001 |
| S3-190847 | Evaluation of EAP-TTLS for non-certificate based UE authentication in SNPNs | Cablelabs, Nokia, Nokia Shanghai Bell | not treated |  |  |
| S3-190848 | Solution on non-certificate based UE authentication in 5G NPN with AAA | Cablelabs, Nokia, Nokia Shanghai Bell | noted |  |  |
| S3-190849 | Solution on non-certificate based UE authentication in 5G NPN without AAA | Cablelabs, Nokia, Nokia Shanghai Bell | noted |  |  |
| S3-190850 | Discussion of security solutions for SNPN service access via PLMN and vice versa | Nokia, Nokia Shanghai Bell | not treated |  |  |
| S3-190851 | Solution on SNPN service access via PLMN | Nokia, Nokia Shanghai Bell | not treated |  |  |
| S3-190852 | Solution on PLMN service access via NPN | Nokia, Nokia Shanghai Bell | not treated |  |  |
| S3-190853 | Discussion on Authentication of UE to PLMN integrated NPN | Nokia, Nokia Shanghai Bell | not treated |  |  |
| S3-190854 | Solution for UE authentication to PLMN integrated NPN | Nokia, Nokia Shanghai Bell | not treated |  |  |
| S3-190855 | KI on credential storage for NPN-Ues | Nokia, Nokia Shanghai Bell | noted |  |  |
| S3-190856 | KI on authentication and authorization of NPN subscribers by a 5G external entity | Nokia, Nokia Shanghai Bell | revised |  | S3-191000 |
| S3-190857 | Rapporteur correction to TR 33819 | Nokia, Nokia Shanghai Bell | approved |  |  |
| S3-190858 | Key issue on secure storage of SNPN access credentials | Samsung, Intel | noted |  |  |
| S3-190859 | Solution for secure storage of SNPN access credentials | Samsung, Intel | noted |  |  |
| S3-190860 | Key issue on CAG access control in Non-standalone NPNs | Samsung | revised |  | S3-190994 |
| S3-190861 | New solution for CAG access control in Non-standalone NPNs  | Samsung | revised |  | S3-190995 |
| S3-190862 | Key issue on Alignment of the terms Private network and NPN | Samsung | noted |  |  |
| S3-190863 | Draft TR 33.xxx - Skeleton TR on Security for NR Integrated Access and Backhaul | Samsung  | approved |  |  |
| S3-190864 | Scope for the study on security for NR Integrated Access and Backhaul | Samsung | revised |  | S3-190916 |
| S3-190865 | Evaluation of Solution #2 | Samsung | noted |  |  |
| S3-190866 | Solution for AS security during RRC Idle mode  | Samsung  | revised |  | S3-190943 |
| S3-190867 | Privacy for Slice Authentication | Lenovo, Motorola Mobility | revised |  | S3-191017 |
| S3-190868 | Solution Evaluations and Conclusion on KI#1 | Lenovo, Motorola Mobility | merged |  | S3-191011 |
| S3-190869 | Security aspects of Service Communication Proxy (SCP) | Nokia, Nokia Shanghai Bell | revised |  | S3-190967 |
| S3-190870 | Solution on Authentication Relay Attack | Lenovo, Motorola Mobility | merged |  | S3-190987 |
| S3-190871 | NF to NF authenticaton and authorization in Indirect communication mode | Nokia, Nokia Shanghai Bell | revised |  | S3-190981 |
| S3-190872 | Authorization of NF service access in SCP | Nokia, Nokia Shanghai Bell | revised |  | S3-190980 |
| S3-190873 | Indirect communication between NFs in roaming scenarios | Nokia, Nokia Shanghai Bell | revised |  | S3-190983 |
| S3-190874 | Service access authorization within a NF Set or NF Service Set | Nokia, Nokia Shanghai Bell | revised |  | S3-190982 |
| S3-190875 | Removal of Editor’s Note in Solution#6 | Lenovo, Motorola Mobility | noted |  |  |
| S3-190876 | Protection of N9 interface in Inter-PLMN scenario | Nokia, Nokia Shanghai Bell | merged |  | S3-190965 |
| S3-190877 | Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN) | Nokia, Nokia Shanghai Bell | revised |  | S3-191013 |
| S3-190878 | Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN) | Nokia, Nokia Shanghai Bell | revised |  | S3-191014 |
| S3-190879 | TLMSP, A Proxy Transport Layer Secure Protocol | NCSC | noted |  |  |
| S3-190880 | (FS\_UP\_IP\_Sec) Integrity protection of the User Plane -New key Issue - Reporting Integrity check failures to the network | BT plc | noted |  |  |
| S3-190881 | Key Issue proposal on location measurement tampering for FS\_eLCS\_Sec | Philips International B.V. | revised |  | S3-190903 |
| S3-190882 | Issue of Alignment of the terms Private network and NPN | SAMSUNG | noted |  |  |
| S3-190883 | The purpose and scope of SCAS | Ericsson | endorsed | S3-190749 | - |
| S3-190884 | SCAS: AMF-specific adaptations of security functional requirements and related test cases | Huawei, Hisilicon | approved | S3-190740 | - |
| S3-190885 | Security Assurance Requirements and Test Case for UPF | Huawei, Hisilicon | approved | S3-190741 | - |
| S3-190886 | ecurity Assurance Requirements and Test Case for UPF- Reference to 33.250 | Huawei, Hisilicon | approved | - | - |
| S3-190887 | Draft TS 33.512 | Deutsche Telekom | approved | - | - |
| S3-190888 | Draft TS 33.513 | Samsung | approved | - | - |
| S3-190889 | Security Assurance Requirement and test cases for SMF | Huawei, Hisilicon | approved | S3-190743 | - |
| S3-190890 | draft TS 33.515 | Huawei | approved | - | - |
| S3-190891 | Test Case: Connection-specific scope of IPX-provider cryptographic material | Deutsche Telekom AG | approved | S3-190728 | - |
| S3-190892 | SCAS SEPP: Serving PLMN ID Mismatch | Nokia, Nokia Shanghai Bell | approved | S3-190780 | - |
| S3-190893 | Draft TS 33.517 | Nokia | approved | - | - |
| S3-190894 | SCAS NEF Add test steps for authorization on northbound APIs | ZTE Corporation | approved | S3-190618 | - |
| S3-190895 | draft TS 33.519 | ZTE | approved | - | - |
| S3-190896 | SCAS 5G: mutual authentication between NFs | Nokia, Nokia Shanghai Bell | approved | S3-190775 | - |
| S3-190897 | Living Document: General SBA/SBI aspects in TS 33.117 | Nokia, Nokia Shanghai Bell | approved | S3-190672 | - |
| S3-190898 | pCR to TR33.814 – Text for Clause Introduction | CATT | approved | S3-190731 | - |
| S3-190899 | Text for Clause 4 Security aspects of eLCS | CATT | approved | S3-190732 | - |
| S3-190900 | pCR to TR33.814 - Key issue for positioning data confidentiality protection | CATT,Huawei | approved | S3-190729 | - |
| S3-190901 | draft TR 33.814 | CATT | approved | - | - |
| S3-190902 | New KI: Privacy control in LCS | Ericsson | approved | S3-190755 | - |
| S3-190903 | Key Issue proposal on location measurement tampering for FS\_eLCS\_Sec | Philips International B.V. | revised | S3-190881 | S3-190959 |
| S3-190904 | New solution: Effective privacy control in LCS | Ericsson | approved | S3-190756 | - |
| S3-190905 | New solution: WLAN measurements from UEs | Ericsson | approved | S3-190751 | - |
| S3-190906 | New solution: Bluetooth measurements from UEs | Ericsson | approved | S3-190752 | - |
| S3-190907 | New solution: TBS measurements from UEs | Ericsson | approved | S3-190754 | - |
| S3-190908 | Draft TR 33.846 | Ericsson | approved | - | - |
| S3-190909 | Key issue to resist the linkability attacks | China Mobile Com. Corporation,ZTE,Huawei | approved | S3-190762 | - |
| S3-190910 | draft TR33.853 | Vodafone | approved | - | - |
| S3-190911 | New key issue on data rate limitation of integrity protection in UP DRB | NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung | revised | S3-190649 | S3-191004 |
| S3-190912 | New key issue on integrity protection capability imbalance in MR-DC scenarios | NEC Europe Ltd | revised | S3-190652 | S3-191019 |
| S3-190913 | pCR: New KI: Integrity Algorithm independence | Qualcomm Incorporated | noted | S3-190802 | - |
| S3-190914 | pCR: New KI: Ability to prioritize certain PDCP packets on the UE uplink | Qualcomm Incorporated | approved | S3-190803 | - |
| S3-190915 | LS on Full date rate support for UP IP | Qualcomm | revised | - | S3-191020 |
| S3-190916 | Scope for the study on security for NR Integrated Access and Backhaul | Samsung | approved | S3-190864 | - |
| S3-190917 | new draft TR 33.XYZ | Samsung | approved | - | - |
| S3-190918 | Scope proposal for eV2X security study | LG Electronics | approved | S3-190770 | - |
| S3-190919 | new draft TR 33.ABC | LG | approved | - | - |
| S3-190920 | Detailed solution 5 in TR 33.935 | Gemalto N.V. | revised | S3-190840 | S3-190955 |
| S3-190921 | Agenda | WG Vice Chair | approved | S3-190600 | - |
| S3-190922 | New KI: Interworking between AKMA and GBA | Ericsson | withdrawn | - | - |
| S3-190923 | draft TR 33.835 | China Mobile | approved | - | - |
| S3-190924 | Key issue on Key freshness in AKMA | Huawei, Hisilicon | approved | S3-190702 | - |
| S3-190925 | Updates to KI #14 | Ericsson | approved | S3-190824 | - |
| S3-190926 | New Solution: Battery efficient AKMA | KPN N.V. | approved | S3-190613 | - |
| S3-190927 | Solution to KI#9 Key separation for AKMA AFs | NEC Europe Ltd | approved | S3-190632 | - |
| S3-190928 | pCR: Reusing KAUSF for AKMA | Qualcomm Incorporated | approved | S3-190801 | - |
| S3-190929 | Solution for Established Key Synchronization | NEC Europe Ltd | approved | S3-190639 | - |
| S3-190930 | Updating solution #16 to include home network option  | NEC Europe Ltd | approved | S3-190644 | - |
| S3-190931 | Resolving Editor's notes in solution 6 | China Mobile Com. Corporation | approved | S3-190774 | - |
| S3-190932 | Solution 15 editorials | Ericsson | approved | S3-190842 | - |
| S3-190933 | Solution 15 comment on the application keys | Ericsson | approved | S3-190843 | - |
| S3-190934 | Way forward on evaluations for FS\_AKMA | ORANGE | endorsed | - | - |
| S3-190935 | Solution 15 evaluation | Ericsson | approved | S3-190844 | - |
| S3-190936 | New security requirement against tampering of RRCResumeRequest message | Huawei, Hisilicon | merged | S3-190669 | S3-190997 |
| S3-190937 | New security requirement against replay of RRCResumeRequest message | Huawei, Hisilicon | revised | S3-190670 | S3-190997 |
| S3-190938 | Adding evaluation for Solution #1 | Apple Computer Trading Co. Ltd | approved | S3-190834 | - |
| S3-190939 | KI#2 in TR 33.809 – updated details (cleanup) | Ericsson | approved | S3-190831 | - |
| S3-190940 | Changing the security requirement for KI #2 | Qualcomm Incorporated | approved | S3-190798 | - |
| S3-190941 | KI#2 in TR 33.809 – new solution for tamper resistant SI messages | Ericsson | approved | S3-190832 | - |
| S3-190942 | Adding evaluation for Solution #2  | Apple Computer Trading Co. Ltd | approved | S3-190835 | - |
| S3-190943 | Solution for AS security during RRC Idle mode  | Samsung  | approved | S3-190866 | - |
| S3-190944 | Updating Key issue #3 for Network detection of nearby false base station | NEC Europe Ltd | approved | S3-190635 | - |
| S3-190945 | KI#3 in TR 33.809 - updates to requirements | Ericsson | approved | S3-190826 | - |
| S3-190946 | Network detection of false base station from UE measurement reports | Nokia | approved | S3-190660 | - |
| S3-190947 | Avoiding UE connecting to fake base station during HO | Huawei, Hisilicon | approved | S3-190665 | - |
| S3-190948 | draft TR 33.813 | Nokia | approved | - | - |
| S3-190950 | draft TR 33.818 | China Mobile | approved | - | - |
| S3-190951 | Considerations on network product class when using NFV technology | China Mobile Com. Corporation | approved | S3-190757 | - |
| S3-190952 | Considerations on SECAM of the virtualized network products | China Mobile Com. Corporation | approved | S3-190758 | - |
| S3-190953 | pCR to 33935 - addition section 4.1 Overview | VODAFONE Group Plc | approved | S3-190768 | - |
| S3-190954 | pCR to 33935 - addition of detailed solution 4b | VODAFONE Group Plc | approved | S3-190773 | - |
| S3-190955 | Detailed solution 5 in TR 33.935 | Gemalto N.V. | approved | S3-190920 | - |
| S3-190956 | draft TR 33.935 | Vodafone | approved | - | - |
| S3-190957 | Conclusion for KDF negotiation for 5G System Security | Huawei, Hisilicon | approved | S3-190723 | - |
| S3-190958 | draft TR 33.808 | Huawei | approved | - | - |
| S3-190959 | Key Issue proposal on location measurement tampering for FS\_eLCS\_Sec | Philips International B.V. | approved | S3-190903 | - |
| S3-190960 | draft TR 33.809 | Apple | approved | - | - |
| S3-190961 | LS on handling of Indirect communication across NF/NF Services | S2-1902905 | replied to | - | - |
| S3-190962 | Discussion on NPN authentication | Huawei, HiSilicon | noted | S3-190700 | - |
| S3-190963 | Reply LS on handling of Indirect communication across NF/NF Services | Deutsche Telekom | approved | - | - |
| S3-190964 | New Key Issue: Support of a UP gateway function on the N9 interface | Ericsson | approved | S3-190744 | - |
| S3-190965 | New KI: flexible protection of data exchange on N9 | Huawei, Hisilicon,Nokia | approved | S3-190737 | - |
| S3-190966 | LS on Clarification of flexibility of N9 protection | Deutsche Telekom | revised | - | S3-191016 |
| S3-190967 | Security aspects of Service Communication Proxy (SCP) | Nokia, Nokia Shanghai Bell,Deutsche Telekom | approved | S3-190869 | - |
| S3-190968 | Key Issue: Secure message transport via the SCP | Deutsche Telekom AG | approved | S3-190727 | - |
| S3-190969 | URLLC-KI UP security performance for low latency | ZTE Corporation | approved | S3-190619 | - |
| S3-190970 | New solution for security for redundant data transmission using Dual Connectivity procedures | Ericsson | approved | S3-190819 | - |
| S3-190971 | URLLC solution5 update | Huawei, HiSilicon,NEC | approved | S3-190682 | - |
| S3-190972 | Dynamic UP security policy control solution for URLLC | Huawei, HiSilicon | approved | S3-190689 | - |
| S3-190973 | Solution #Y: Security for redundant data transmission using Dual Connectivity | Ericsson | approved | S3-190818 | - |
| S3-190974 | solution1 and evaluation update | Huawei, HiSilicon | approved | S3-190685 | - |
| S3-190975 | deleting the EN of solution3 | Huawei, HiSilicon | approved | S3-190680 | - |
| S3-190976 | evaluation of solution 3 | Huawei, HiSilicon | approved | S3-190683 | - |
| S3-190977 | solution 2 clarification | Huawei, HiSilicon | approved | S3-190679 | - |
| S3-190978 | Security Assurance Requirement and Test for NRF | Huawei, Hisilicon | noted | S3-190742 | - |
| S3-190979 | draft TR 33.825 | Huawei | approved | - | - |
| S3-190980 | Authorization of NF service access in SCP | Nokia, Nokia Shanghai Bell | approved | S3-190872 | - |
| S3-190981 | NF to NF authenticaton and authorization in Indirect communication mode | Nokia, Nokia Shanghai Bell | approved | S3-190871 | - |
| S3-190982 | Service access authorization within a NF Set or NF Service Set | Nokia, Nokia Shanghai Bell | approved | S3-190874 | - |
| S3-190983 | Indirect communication between NFs in roaming scenarios | Nokia, Nokia Shanghai Bell | approved | S3-190873 | - |
| S3-190984 | Key Issue: Handling of invalid IPX patches | Deutsche Telekom AG | approved | S3-190725 | - |
| S3-190985 | KI#3 in TR 33.809 - new solution for enriched measurement reports | Ericsson,Huawei | approved | S3-190827 | - |
| S3-190986 | New requirment for Authentication relay attack | Huawei, Hisilicon | approved | S3-190733 | - |
| S3-190987 | New solution for Authentication relay attack | Huawei, Hisilicon | approved | S3-190734 | - |
| S3-190988 | Protection against Man-in-the-Middle false base station attacks | Qualcomm Incorporated | revised | S3-190793 | S3-191021 |
| S3-190989 | References to TR 33.809 | BT | approved | - | - |
| S3-190990 | NPN authentication way forward | ORANGE | revised | - | S3-190999 |
| S3-190991 | Proposed solution to the key hierarchy for non-public networks | Qualcomm Incorporated | approved | S3-190787 | - |
| S3-190992 | Proposed addition to key issue#1.1 for standalone non-public networks | Qualcomm Incorporated | approved | S3-190788 | - |
| S3-190993 | Adding network binding requirement to the keys issue #1.1 on standalone public networks | Qualcomm Incorporated | approved | S3-190789 | - |
| S3-190994 | Key issue on CAG access control in Non-standalone NPNs | Samsung | approved | S3-190860 | - |
| S3-190995 | New solution for CAG access control in Non-standalone NPNs  | Samsung | approved | S3-190861 | - |
| S3-190996 | Creating a combined solution for usage of KSEAF and KAUSF  | NEC Europe Ltd | approved | S3-190645 | - |
| S3-190997 | New security requirement against replay of RRCResumeRequest message | Huawei, Hisilicon | approved | S3-190937 | - |
| S3-190998 | Notifying cell information to the network after authentication procedure failure | NEC Europe Ltd | revised | S3-190654 | S3-191006 |
| S3-190999 | NPN authentication way forward | ORANGE | revised | S3-190990 | S3-191003 |
| S3-191000 | KI on authentication and authorization of NPN subscribers by a 5G external entity | Nokia, Nokia Shanghai Bell | approved | S3-190856 | - |
| S3-191001 | Deployment options for authentication in NPNs | Cablelabs, Nokia, Nokia Shanghai Bell | approved | S3-190846 | - |
| S3-191002 | Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN | InterDigital, Inc. | approved | S3-190609 | - |
| S3-191003 | NPN authentication way forward | ORANGE | endorsed | S3-190999 | - |
| S3-191004 | New key issue on data rate limitation of integrity protection in UP DRB | NEC Europe Ltd, Lenovo, Motorola Mobility, Samsung | approved | S3-190911 | - |
| S3-191005 | Solution for Key freshness in AKMA | Huawei, Hisilicon | approved | S3-190703 | - |
| S3-191006 | Notifying cell information to the network after authentication procedure failure | NEC Europe Ltd | noted | S3-190998 | - |
| S3-191007 | Amendment to solution #3 | Huawei, HiSilicon | approved | S3-190698 | - |
| S3-191008 | Remove EN in 6.6.3 | Huawei, Hisilicon | approved | S3-190738 | - |
| S3-191009 | Solution for slice specific authorization | Huawei, Hisilicon | approved | S3-190739 | - |
| S3-191010 | Proposed evaluation for Solution #1 AS and NAS security for RLOS services | Qualcomm Incorporated | approved | S3-190781 | - |
| S3-191011 | Proposed update for Solution #2 AS and NAS security based on the emergency call procedures | Qualcomm Incorporated,Lenovo | approved | S3-190783 | - |
| S3-191012 | New KI: N3GPP Key Hierarchy | Ericsson | approved | S3-190745 | - |
| S3-191013 | Mobility between TNAPs within the Trusted Non-3GPP Access Network (TNAN) | Nokia, Nokia Shanghai Bell | approved | S3-190877 | - |
| S3-191014 | Mobility between TNGFs within the Trusted Non-3GPP Access Network (TNAN) | Nokia, Nokia Shanghai Bell | approved | S3-190878 | - |
| S3-191015 | draft TR 33.807 | Huawei | approved | - | - |
| S3-191016 | LS on Clarification of flexibility of N9 protection | Deutsche Telekom | approved | S3-190966 | - |
| S3-191017 | Privacy for Slice Authentication | Lenovo, Motorola Mobility | revised | S3-190867 | S3-191034 |
| S3-191018 | draft TR 33.819 | Nokia | approved | - | - |
| S3-191019 | New key issue on integrity protection capability imbalance in MR-DC scenarios | NEC Europe Ltd,Huawei | approved | S3-190912 | - |
| S3-191020 | LS on Full date rate support for UP IP | Qualcomm | approved | S3-190915 | - |
| S3-191021 | Protection against Man-in-the-Middle false base station attacks | Qualcomm Incorporated | approved | S3-190988 | - |
| S3-191022 | Draft skeleton document for TR 33.935 | Vodafone | revised | - | S3-191024 |
| S3-191023 | draft TR 33.815 | Sprint | approved | - | - |
| S3-191024 | Draft skeleton document for TR 33.935 | Vodafone | approved | S3-191022 | - |
| S3-191025 | Deleting EN on the usage of per-gNB and per-UE counters for solution #7 “protecting gNB from RRC DoS attack” | Huawei, Hisilicon | approved | S3-190661 | - |
| S3-191026 | draft TR 33.861 | Ericsson | approved | - | - |
| S3-191027 | Solution proposal for FS\_CIoT\_sec\_5G key issue #1 and #2 | Philips International B.V. | approved | S3-190603 | - |
| S3-191028 | Solution to identify misbehaving UEs | Huawei, Hisilicon | approved | S3-190704 | - |
| S3-191029 | Solution to Migitate DDoS Attack based on RAN | Huawei, Hisilicon | approved | S3-190705 | - |
| S3-191030 | New Solution: Key separation for untrusted and trusted access | Ericsson | approved | S3-190747 | - |
| S3-191031 | Draft TR 33.855 | Deutsche Telekom | approved | - | - |
| S3-191032 | Adding an evaluation to solution #9 in TR 33.861 | Qualcomm Incorporated | approved | S3-190800 | - |
| S3-191033 | Adding an evaluation to solution #10 in TR 33.861 | Qualcomm Incorporated | approved | S3-190786 | - |
| S3-191034 | Privacy for Slice Authentication | Lenovo, Motorola Mobility | approved | S3-191017 | - |
| S3-191035 | Work Plan input from Rapporteurs | WG Vice Chairs | noted | S3-190612 | - |

## Annex B: Lists of liaisons

### B1: Incoming liaison statements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document | Original | Title | From | Decision | Reply TDoc |
| S3-190610 |  | Initialisation of Sensitive Functions in a Virtualised Environment | ETSI TC CYBER | noted | (none) |
| S3-190611 |  | Reply LS on authentication of group of IoT devices | S1-190501 | postponed | (none) |
| S3-190961 |  | LS on handling of Indirect communication across NF/NF Services | S2-1902905 | replied to | S3-190963 |

### B2: Outgoing liaison statements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document | Title | To | Cc | reply to i/c LS |
| S3-190963 | Reply LS on handling of Indirect communication across NF/NF Services | SA2 | - | S3-190961 |
| S3-191016 | LS on Clarification of flexibility of N9 protection | GSMA 5GJA | - | - |
| S3-191020 | LS on Full date rate support for UP IP | RAN2 | RAN, RAN1, RAN3 | - |

## Annex C: List of draft Technical Specifications and Reports

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Spec | vers | Doc title |
| S3-190887 | 33.512 | 0.6.0 | Draft TS 33.512 |
| S3-190888 | 33.513 | 0.3.0 | Draft TS 33.513 |
| S3-190890 | 33.515 | 0.2.0 | draft TS 33.515 |
| S3-190893 | 33.517 | 0.3.0 | Draft TS 33.517 |
| S3-190895 | 33.519 | 0.4.0 | draft TS 33.519 |
| S3-190901 | 33.814 | 0.3.0 | draft TR 33.814 |
| S3-190908 | 33.846 | 0.1.0 | Draft TR 33.846 |
| S3-190910 | 33.853 | 0.2.0 | draft TR33.853 |
| S3-190923 | 33.835 | 0.4.0 | draft TR 33.835 |
| S3-190948 | 33.813 | 0.3.0 | draft TR 33.813 |
| S3-190950 | 33.818 | 0.2.0 | draft TR 33.818 |
| S3-190956 | 33.935 | 0.1.0 | draft TR 33.935 |
| S3-190958 | 33.808 | 0.3.0 | draft TR 33.808 |
| S3-190960 | 33.809 | 0.3.0 | draft TR 33.809 |
| S3-190979 | 33.825 | 0.4.0 | draft TR 33.825 |
| S3-191015 | 33.807 | 0.4.0 | draft TR 33.807 |
| S3-191018 | 33.819 | 0.3.0 | draft TR 33.819 |
| S3-191022 | 33.935 | 0.0.0 | Draft skeleton document for TR 33.935 |
| S3-191023 | 33.815 | 0.4.0 | draft TR 33.815 |
| S3-191024 | 33.935 | 0.0.0 | Draft skeleton document for TR 33.935 |
| S3-191026 | 33.861 | 0.5.0 | draft TR 33.861 |
| S3-191031 | 33.855 | 1.4.0 | Draft TR 33.855 |

## Annex D: List of participants

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| TITLE | Family Name | Given Name | Employer Organization | Employer Category Code | Organization Represented | Organization Represented Category Code |
| Dr. | Aldén | Magnus | Telia Company AB | ETSI | Telia Company AB | ETSI |
| Dr. | Ben Henda | Noamen | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Mr. | Bernsen | John | Philips International B.V. | ETSI | Philips International B.V. | ETSI |
| Mr. | Blanchard | Colin | BT plc | ETSI | BT plc | ETSI |
| Mr. | Brusilovsky | Alec | InterDigital, Inc. | ETSI | InterDigital, Inc. | ETSI |
| Mr. | Canterbury | Mark | Tencastle Limited | National Technical Assistance | ETSI |
| Mr. | Castagno | Mauro | TELECOM ITALIA S.p.A. | ETSI | TELECOM ITALIA S.p.A. | ETSI |
| Mr. | Cichonski | Jeffrey | NIST | ATIS | NIST | ATIS |
| Mr. | De Kievit | Sander | NEC Corporation | ETSI | NEC Corporation | ETSI |
| Ms. | Deng | Juan | HuaWei Technologies Co., Ltd | CCSA | Huawei Telecommunication India | TSDSI |
| Mr. | Doerr | Johannes | BMWi | ETSI | BMWi | ETSI |
| Miss | Driscoll | Florence | NCSC | ETSI | NCSC | ETSI |
| Dr. | Eriksson | Roger | ADVENICA AB | NCSC | ETSI |
| Dr. | Escott | Adrian | Qualcomm CDMA Technologies | ETSI | Qualcomm CDMA Technologies | ETSI |
| Mr. | Evans | Tim P. | VODAFONE Group Plc | ETSI | VODAFONE Group Plc | ETSI |
| Mr. | Gaarder | Klaus | TELENOR ASA | ETSI | TELENOR ASA | ETSI |
| Mr. | Gamishev | Todor | Orange | ETSI | Orange | ETSI |
| Mr. | Guo | Longhua | HUAWEI TECH. GmbH | ETSI | HUAWEI TECH. GmbH | ETSI |
| Ms. | Guo | Shu | Apple Computer Trading Co. Ltd | CCSA | Apple Computer Trading Co. Ltd | CCSA |
| Mr. | Hanhisalo | Markus | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Dr. | Huang | Lin | Qihoo 360 | CCSA | Qihoo 360 | CCSA |
| Miss | Huang | Xiaoting | China Mobile Com. Corporation | CCSA | China Mobile Com. Corporation | CCSA |
| Miss | Jerichow | Anja | Nokia Germany | ETSI | Nokia Germany | ETSI |
| Dr. | Jost | Christine | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Dr. | Keesmaat | Iko | TNO | ETSI | TNO | ETSI |
| Dr. | Kim | Joonwoong | LG Electronics France | ETSI | LG Electronics France | ETSI |
| Mr. | Kohalmi | Steve | Juniper Networks | ETSI | Juniper Networks | ETSI |
| Mr. | Kolekar | Abhijeet | Intel Corporation (UK) Ltd | ETSI | Intel Mobile Communications | TSDSI |
| Dr. | Kunz | Andreas | Motorola Mobility Germany GmbH | ETSI | Lenovo (Beijing) Ltd | CCSA |
| Mr. | Leadbeater | Alex | BT plc | ETSI | BT plc | ETSI |
| Dr. | Lee | Soo Bum | Qualcomm Incorporated | ATIS | Qualcomm Incorporated | ATIS |
| Dr. | Lei | Zander (Zhongding) | HuaWei Technologies Co., Ltd | CCSA | Huawei Technologies Co. Ltd. | ETSI |
| Miss | Lu | Wei | Nokia Korea | TTA | Nokia Shanghai Bell | CCSA |
| Mr. | McKee | Alan | NCSC | ETSI | NCSC | ETSI |
| Mr. | Mellqvist | Anders | Sony Europe Limited | ETSI | Sony Mobile Communications | ARIB |
| Dr. | Muhanna | Ahmad | Huawei Technologies Sweden AB | ETSI | Huawei Technologies Sweden AB | ETSI |
| Mr. | Nair | Suresh | Nokia Germany | ETSI | Nokia | ATIS |
| Mr. | Nakarmi | Prajwol Kumar | Ericsson Limited | ETSI | Ericsson Limited | ETSI |
| Mr. | Naslund | Mats | NDRE | ETSI | NDRE | ETSI |
| Mr. | Normann | Henrik Andreas | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Mr. | Oishi | Tateo | Sony Europe Limited | ETSI | Sony Corporation | ARIB |
| Mr. | Palanigounder | Anand | Qualcomm UK Ltd | ETSI | Qualcomm Incorporated | ATIS |
| Mrs. | Pauliac | Mireille | Gemalto N.V. | ETSI | Gemalto N.V. | ETSI |
| Mr. | PENG | Jin | ZTE Corporation | ETSI | Nubia Technology Co.,Ltd | CCSA |
| Mr. | Rajadurai | Rajavelsamy | Samsung R&D Institute UK | ETSI | Samsung R&D Institute UK | ETSI |
| Mrs. | Rong | Wu | Huawei Technologies Co. Ltd. | ETSI | Huawei Technologies Co. Ltd. | ETSI |
| Mr. | Rudolph | Hans Christian | Deutsche Telekom AG | ETSI | Deutsche Telekom AG | ETSI |
| Mr. | Schumacher | Greg | SPRINT Corporation | ETSI | SPRINT Corporation | ETSI |
| Mr. | Tangudu | Narendranath Durga | Samsung R&D Institute India | TSDSI | SAMSUNG R&D INSTITUTE JAPAN | ARIB |
| Mr. | Tiwari | Kundan | NEC Corporation | TTC | NEC Corporation | ARIB |
| Mr. | Toor | Gurbakshish Singh | TD Tech Ltd | CCSA | TD Tech Ltd | CCSA |
| Dr. | Tsiatsis | Vlasios | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Mrs. | Vahidi | Helena | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Mr. | Vujcic | Dragan | IDEMIA | ETSI | IDEMIA | ETSI |
| Mr. | Whorlow | Colin | NCSC | ETSI | HOME OFFICE | ETSI |
| Ms. | Wifvesson | Monica | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Mr. | Wong | Marcus | Huawei Tech.(UK) Co., Ltd | ETSI | Huawei Technologies (Korea) | TTA |
| Dr. | Wong | Stan | GSM Association | OTHER | GSM Association | OTHER |
| Mr. | Woodward | Tim | Motorola Solutions Danmark A/S | ETSI | Motorola Solutions UK Ltd. | ETSI |
| Mr. | Xie | Zhenhua | ZTE Corporation | ETSI | ZTE Corporation | ETSI |
| Miss | Xu | Hui | CATT | ETSI | CATT | ETSI |
| Dr. | Zhang | Bo | Huawei Technologies Co. Ltd. | ETSI | Huawei Technologies Co. Ltd. | ETSI |
| Miss | Zhang | Xiaowei | Deutsche Telekom AG | ETSI | Deutsche Telekom AG | ETSI |
| Mr. | Zhou | Wei | CATT | CCSA | CATT | CCSA |
| Dr. | Zugenmaier | Alf | NTT DOCOMO INC. | TTC | NTT DOCOMO INC. | TTC |

## Annex E: List of future meetings

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | Start date | End date (OP) | Town | Country | Reference |
| SA3#95 | 2019-05-06 | 2019-05-10 | Reno | US | S3-95 |
| SA3-Ad-Hoc | 2019-06-24 | 2019-06-28 | Sapporo | JP | S3-ah-40149 |
| SA3#96 | 2019-08-26 | 2019-08-30 | Wroclaw | PL | S3-96 |
| SA3-Ad-Hoc | 2019-10-14 | 2019-10-18 | TBD | CN | S3-ah-40150 |
| SA3#97 | 2019-11-18 | 2019-11-22 | Reno | US | S3-97 |