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

 **Meeting Report
for
TSG SA WG3
meeting: 92-AdHoc**

**Harbin, China, 24/09/2018 to 28/09/2018**

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 3

4.1 Security aspects of 5G System - Phase 1 (5GS\_Ph1-SEC) (Rel-15) 3

4.1.1 Key hierarchy 3

4.1.2 Key derivation 4

4.1.3 Mobility 6

4.1.4 AS security 6

4.1.5 NAS security 14

4.1.6 Security context 20

4.1.7 Visibility and Configurability 20

4.1.8 Primary authentication 20

4.1.9 Secondary authentication 22

4.1.10 Interworking 22

4.1.11 non-3GPP access 26

4.1.12 NDS 27

4.1.13 Service based architecture 29

4.1.13.1 Interconnect (SEPP related) 29

4.1.13.2 Other 35

4.1.14 Privacy 37

4.1.15 Incoming and outgoing Lses 40

4.1.16 Others 46

4.2 Security Assurance Specification for 5G (SCAS\_5G) (Rel-16) 50

4.2.1 NR Node B (gNB) (TS 33.511) 50

4.2.2 Access and Mobility Management Function (TS 33.512) 55

4.2.3 User Plane Function (UPF) (TS 33.513) 57

4.2.4 Unified Data Management (UDM) (TS 33.514) 59

4.2.5 Session Management Function (SMF) (TS 33.515) 61

5 Studies 61

5.1 Security aspects of single radio voice continuity from 5G to UTRAN (FS\_5G\_UTRAN\_SEC) (Rel-16) 61

5.2 Study on evolution of Cellular IoT security for the 5G System (FS\_CIoT\_sec\_5G) (Rel-16) 63

5.3 Study on the security of the Wireless and Wireline Convergence for the 5G system architecture (FS\_5WWC\_SEC) (Rel-16) 76

5.4 Study on Security Aspects of PARLOS (FS\_PARLOS\_Sec) (Rel-16) 84

5.5 Study on authentication and key management for applications based on 3GPP credential in 5G IoT (FS\_AKMA) (Rel-16) 90

5.6 Study on Security Aspects of the 5G Service Based Architecture (FS\_SBA-Sec) (Rel-16) 99

5.7 Study on Long Term Key Update Procedures (FS\_LTKUP) (Rel-16) 101

5.8 Study on Supporting 256-bit Algorithms for 5G (FS\_256-Algorithms) (Rel-16) 102

6 Any Other Business 104

Annex A: List of contribution documents 108

Annex B: List of change requests 119

Annex C: Lists of liaisons 120

C1: Incoming liaison statements 120

C2: Outgoing liaison statements 120

Annex D: List of draft Technical Specifications and Reports 121

Annex G: List of participants 121

Annex H: List of future meetings 123

## 1 Opening of the meeting

## 2 Approval of Agenda and Meeting Objectives

**S3-182800 Agenda**

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

**Discussion:**

Numbering was according to MCC's tdoc sheet, as there was a typo in the agenda: twice 4.1.4 and 4.1.5.

No revision number required.

Anand read IPR and Anti-Trust Law reminder

**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.

## 4 Work Areas

### 4.1 Security aspects of 5G System - Phase 1 (5GS\_Ph1-SEC) (Rel-15)

#### 4.1.1 Key hierarchy

**S3-182953 Clarification to key hierarchy description**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

QC: what is the value of having the statement, AUSF is always in home network

Nokia: these questions come up all the time

Orange: agree with QC

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

**S3-182956 Clarification to support of authentication methods**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182680)

**Discussion:**

QC: current normative text is ok, Note not necessary, but ok.

VF: why UE, not ME.

Orange: ok with first sentence of note, second sentence not required, because it doesn't need to be stored

E//: AUSF doesn't need to support both methods with this change? needs to support

NEC: support E// view

Huawei: last sentence of note 2b should go

Idemia: operator decision also in UICC

Orange: UE and network shall support EAP-AKA' and 5G-AKA

Nokia: idea is to explain what is mandated

Tmobile:

DCM: list network functions

Orange: AMF, SEAF, UDM, etc

E//: AUSF needs to support EAP framework

Nokia: note 2b: It is home operators decision which authentication method is selected

E//: this is already state in authentation procedure

**Decision:** The document was **revised to S3-183077**.

**S3-183077 Clarification to support of authentication methods**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182956)

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

#### 4.1.2 Key derivation

**S3-182955 Clarification to AUSF key derivation**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

DCM: Should "exclusive or' become XOR - agreed - approved as S3-183097

**Decision:** The document was **revised to S3-183097**.

**S3-183097 Clarification to AUSF key derivation**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182955)

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

**S3-182958 Alignment regarding KEY reference to 33.220**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Vdf: Note needs editorial reword - taken offline - revised to S3-183098

**Decision:** The document was **revised to S3-183098**.

**S3-183098 Alignment regarding KEY reference to 33.220**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182958)

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

**S3-182959 Misleading text with reference regarding serving network name**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Vdf: 'the' was deleted by mistake in several places - taken for offline discussion

E//: serving network name and SN ID defined terms

revert

-> revised in S3-183099

**Decision:** The document was **revised to S3-183099**.

**S3-183099 Misleading text with reference regarding serving network name**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182959)

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

**S3-182960 Clarification on first bits of EMSK**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

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

**S3-183061 draft TS 33.512**

 *Type: draft TS For: Approval
 33.512 v0.3.0
 Source: Deutsche Telekom*

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

#### 4.1.3 Mobility

**S3-182889 key isolation between AMFs when UDSF is deployed**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

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

**S3-183027 Mobility – Clarification of downlink NAS COUNT in N2 handover**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

It is proposed to clarify that the source AMF shall always increment the downlink NAS COUNT by one, after sending off the Namf\_Communication\_CreateUEContext Request message.

**Discussion:**

It is proposed to clarify that the source AMF shall always increment the downlink NAS COUNT by one, after sending off the Namf\_Communication\_CreateUEContext Request message.

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

#### 4.1.4 AS security

**S3-182802 The exposed I-RNTI issues in RRC resume procedure**

 *Type: discussion For: Decision
 Source: OPPO*

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

**S3-182851 RRC Resume Request Authentication Token Calculation**

 *Type: discussion For: Endorsement
 33.501 v..
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

E//: E// have a CR for proposal 1 as well. Support that this type confusion attack needs to be solved.

Samsung: proposal 1 already decided

E//: resume constant would prevent type confusion attack

Nokia: is this a valid attack

on Proposal #2

E//: multiple options exist, but Resume cause is not unique, so it is not valid solution

Samsung: agree with E//

QC: but it is a solution to type confusion in case that is the only place this token is included

E//: look at complete integrity protection in R16

Huawei: then reword proposal

proposal 3

QC: in terms of included identity, prefer option 2

E//: revisit this in R16

Huawei: but there is an issue now

QC: there is confusion possible, and no impact on ASN.1

Samsung: maybe too late for R15, there is an attack, but not severe enough

E//: agree

Nokia: in case of an attack, UE goes thorugh active mode.

QC: use I-RNTI would avoid change to C-RNTI calculation in RAN.

no agreement

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

**S3-182852 Update ResumeMAC-I calculation**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

together with 853

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

**S3-182853 Update RNA Update Procedure Security**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

QC: some of the text is independent, so text about not relocation is fine

E//: this is agreeable, but use of resume constant is not in there

Nokia: this is agreeable

kept open, together with 860

discussed independently after offline

QC: should there be a note saying that there is still a change in the key because there is a NCC value sent.

Huawei: clear, no note required.

Approved

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

**S3-182854 Dual Connectivity Structure Update**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

E//: should be under introduction

Huawei: parallel to E// contribution in RAN2

E//: will there be redundant text

Huawei: only differences going in the section

QC: architecture picture is easy, but if there is next to no difference, then keep it in the existing text

E//: if delta is big, then use Huawei way, otherwise do it the QC way.

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

**S3-182855 Intra-gNB-CU term synchronization**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon,*

**Discussion:**

Huawei presents

E//: not correct baseline, need to see on real baseline

Huawei: ok, come back with correct baseline

E//: separation of intra-gNB CU and other intra gNB handovers is confusing

Huawei: then add note. In RAN spec there is no intra gNB handover.

kept open

Nokia: check for name of handover is ok

approved

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

**S3-182859 Update RRC reestablishment security procedure based on RAN2 agreement**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

E//: work on this until next meeting

QC: need alignment with RAN spec

postponed

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

**S3-182860 DRAFT LS on ResumeMAC-I Calculation for RRC Resume Request**

 *Type: LS out For: Approval
 to RAN2 and RAN3
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Huawei: Two issue need to be covered: type confusion and a DoS attack, further resume MAC-I Calculation

E//: two solutions can be sent to RAN, but MAC-I calculation is not necessary as there is no integrity protection requirement

QC: is it an attack or is it that the UE is not knowing the parameters

E//: type confusion is a problem, might be an attack, but desynchronization is not really an attack, but use of token that is used for UE identification for integrity can be looked at for R16. security attack is not clear to E//

Huawei: There is security attack for the UE requesting resume for an emergency call the UE can cause a denial of service attack

E//: this may be a more generic attack

Samsung: agree, e.g. the attacker could send a reject

this was taken offline.

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

**S3-183105 DRAFT LS on ResumeMAC-I Calculation for RRC Resume Request**

 *Type: LS out For: Approval
 to RAN2 and RAN3
 Source: Huawei, Hisilicon*

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

**S3-182861 N2 HO: Handling source algorithms for RRC Reestablishment procedure**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Nokia: decipher and … which is deleted is still correct

Huawei: refer to complete procedure

QC: base text may be incorrect

DCM: do we need formal way of checking, ie LS or action item

QC: under the assumption we have this, then the text is acceptable

approved

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

**S3-182894 Involve Fresh Parameters to Input of InactiveMAC-I to Avoid Replay Attack**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

noted according to discussion in 3024

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

**S3-182897 RRC Reestablishment security handling when N2 Handover happens**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

E//: is reestablishment supported for N2, not clear.

QC: same comment. Is AMF preparing multiple gNBs?

Huawei: if in N2 multiple KNG-RAN\*s are discarded, they are prepared

QC: no, keys are not used at all,

Huawei: then second paragraph needs to be clarified

QC: need to check with RAN2 colleagues

noted

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

**S3-182917 UP security policy in NN-DC and MR-DC**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

QC: take together with 995 and 3025

**Decision:** The document was **revised to S3-183106**.

**S3-183106 UP security policy in NN-DC and MR-DC**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon, Qualcomm Incorporated, and Ericsson*

(Replaces S3-182917)

**Discussion:**

Huawei presents draft

E//: more time

kept open

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

**S3-182969 The exposed I-RNTI issues in RRC resume procedure**

 *Type: discussion For: Approval
 Source: OPPO*

**Abstract:**

This DP discuss the exposed I-RNTI issues in RRC resume procedure.

**Discussion:**

OPPO presents

Nokia: would reassigning I-RNTI work

E//: I-RNTI is temporary identifier, and soemtimes the gNB rejects UEs without knowing the identifier of UE

Apple: I-RNTI consists of AMF-ID and cell-ID without fixed length, so there is now security issue

E//: for tracking UEs, the new RNTI is sent encrypted

CMCC: only issue if temporary identifier is used for days

Huawei: reject is done when gNB doesn't have context, so there is no way to send new I-RNTI protect. Further, there is no issue

Agreement: there is no security issue

noted

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

**S3-182993 RRC Inactive security issue**

 *Type: discussion For: Discussion
 Source: Qualcomm Incorporated*

**Discussion:**

QC presents

together with 994 and 3045

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

**S3-182994 Key derivation in the RRC Inactive state**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Qualcomm Incorporated*

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

**S3-182995 MR-DC user plane integrity protection**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Qualcomm Incorporated*

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

**S3-183023 AS sec – preventing "type confusion" attack between resume and re-establishment procedures**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

This contribution proposes to have type separation between resumeMAC-I and shortMAC-I.

**Discussion:**

E// presents

Huawei: this is possibility, so send both to RAN2?

Kept open, together with 852

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

**S3-183024 AS sec – discussion on replay protection of inactiveMAC-I**

 *Type: discussion For: Endorsement
 33.501 v..
 Source: Ericsson*

**Abstract:**

This discussion proposes that SA3 gives secure options to choose from

**Discussion:**

E// presents

QC: this is not a security problem worth solving, attacker can just reject the UE, and none of the solutions address this

Huawei: agree with QC somehow, even a replay with a temporary C-RNTI is possible.If the resume complete is not sent, then the gNB won't relocate the UE.

E//: this is about replay attack?

QC: Solution is not dealing with all variants of attack, and the implementation is really difficult as it going across the stack

Huawei: if LS is sent to RAN, then just give only one solution

E//: there was a conclusion last meeting ago to try to address this, so we need to send an LS to RAN2 to tell them that we are not addressing this problem

There will be an LS in 3059 on Replay protection -> Noamen

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

**S3-183025 AS sec – integrity protection of traffic between UE and SN**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

This contribution proposes that user plane integrity protection is "supported" in SN for NGEN-DC if DRBs in SN has a separate PDU session.

**Discussion:**

E// presents

VF: after a handover to eNB and back to gNB, will there still be integrity protection

E//: mobility handled differently

Huawei: master node may move bearer from gNB to ng-eNB.

E//: possibility for stationary UE

QC: even stationary gNB may be haded over. Complexity for this is high, introduce when integity for ng-eNB is introduced in a later release.

Nokia: not support, but is not used.

DCM: it should be about use, not about support, so wrong place to document this.

E//: support is not question, but usage, request to do this until Spokane meeting

E//: agree that for dual connectivity, for MRDC, UP integrity protection will not be used for SN.

QC: time critical because RAN is working on this

merge 917 and 995, note 3025

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

**S3-183045 Comments on RRC Inactive security issue**

 *Type: discussion For: (not specified)
 33.501 v..
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Nokia: use different NCC value can also work?

Huawei: NCC is not available

E//: disagree on the proposal, rare scenario and feature is optional, network can take specific action for this scenario, gNB can do the relocation to avoid this scenario, similar discussion in previous meeting

Samsung: can be handled by implementation

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

**S3-183059 LS on replay protection**

 *Type: LS out For: Approval
 to RAN2, cc RAN3
 Source: Ericsson*

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

**S3-183143 LS RRC Reestablishment during N2 handover**

 *Type: LS out For: Approval
 to RAN2, cc RAN3
 Source: Huawei*

**Discussion:**

Huawei presents draft

E//: remove the possible change description

approved

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

#### 4.1.5 NAS security

**S3-182830 Modification on NAS SMC during multiple registrations in the same PLMN**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: CATT*

**Discussion:**

CATT presents

E//: not needed, was discussed previously, because access type is fixed

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

**S3-182887 Clarification on length of the ABBA parameter**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

QC: this was discussed in the last two meetings, it was agreed as variable length

Huawei: length needs to signalled

E//: length of parameter is limited

Nokia: fixed length is easier, but variable can also be handled.

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

**S3-182937 Transmission mechanism of SUCI in NAS procedure**

 *Type: discussion For: Endorsement
 33.501 v..
 Source: NEC Europe Ltd*

**Abstract:**

It is proposed that SA3 endorses the proposal in this discussion.

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

**S3-182941 SUCI freshness in registration procedure**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: NEC Europe Ltd*

**Abstract:**

CR to clarify freshness of SUCI in registration procedure.

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

**S3-183026 NAS key refresh**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

It is proposed that if the AMF determines that NAS key refresh is required , the AMF and the UE may derive a new KAMF key using horizontal KAMF derivation using the current uplink NAS COUNT as described in clause 6.9.3 for mobility update registration.

**Discussion:**

E// presents

Huawei: horizontal KAMF is used for AMF change, is this needed here?

E//: correct, but NAS key change needs to be initiated, reuse mechanism

QC: small difference because use of last NAS uplink, the value could be different between network and UE, tie to initial NAS messages

E//: ok with tie to initial NAS message

Nokia: what is the initial NAS message

E//: registration, etc.

Huawei: not clear that the paragraph was previously agreed on. Derive new KAMF, and not clear it deals with multi-NAS

QC: restrict to happen during registration or service request procedure

E//: no special UE handling required

QC: not clear from text,

E//: which inital NAS message, mention authentication, add text related to timing.

**Decision:** The document was **revised to S3-183075**.

**S3-183075 NAS key refresh**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

(Replaces S3-183026)

**Discussion:**

E// presents draft

E// presents v2

Nokia: delete editor's note

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

**S3-183040 Modification of initial NAS message protection**

 *Type: draftCR For: Approval
 33.501 v15.2.0
 Source: ZTE Corporation*

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

**S3-183041 Initial NAS – Discussion on Initial NAS protection**

 *Type: discussion For: Endorsement
 Source: Intel Corporation (UK) Ltd*

**Discussion:**

Intel presents

E//: refer to partial ciphering, start from there, don't start from protecting all elements

QC: technical issues with the papers have technical issues, home public key may not always be there, distribution of serving network public key is not defined.

Intel: without home public key, SUPI is sent in clear anyways, used only for elements in clear.

QC: VF wants to provide privacy without public keys

VF: some networks want to use with a LTE USIM, so no public key

Huawei: in SA plenary, whole message needed to be protected.

Nokia: plenary did not ask to protect everything,

Orange: NSSAI was agreed to go in clear to avoid goign to home for AMF sleection

ATT: impression: all messages need to be protected, unless there is a good reason such as routing etc. Further important to keep timeline. From practical point, encrypt and keep routing info in clear is good for R15.

NEC: start with huawei

DCM: good start for analysis of how to protect complete message, but there are technical problems, timeline problems with both solutions, so go forward with partial NAS protection.

CMCC: some USIMs can not easily be updated, so go forward with partial NAS solution

Gemalto: we could still mandate a 5G USIM

CMCC: but what to do with legacy USIM subscribers

BT: there was a show of hands for privacy, public key for serving network was rejected due to complexity

Orange: SA1 requirement is saying for security reasons.

Nokia: In 23.501: some elements are necessary in clear, but NSSAI in RAN there may be way not to have it in clear.

E//: LS from SA2 has the list of elements that need to be in the clear.

ATT: plenary said everything to be encrypted, unless justified to be in the clear.

BT: agree, move elements into unprotected part only as exception

E//:agree with that, but move only to protected when privacy sensitive

BT: no, the other way round.

Huawei: SA plenary, not go back to SA2 opinion. If current solution doesn't work, then propose new solutions

E//: not possible in this timeframe

Orange: some companies said that it is not possible

Huawei: 20+ operators wanted this in plenary

E//: is the solution feasible

DCM: trade-off: between security and performance, make a working assumption to go with partial ciphering

Huawei: SA3 can't make this decision

DCM: someone has to

BT: SA plenary has instructed us to decide

ATT: need to consider time scale

QC: SA plenary says to take existing solution as basis.

BT: is it clear that serving network public key is a global PKI.

Nokia: except the bare minimum all is encrypted

QC: go offline with this

BT: if NSSAI is not in the exception list, then the benchmark should be if the IEs are essentially identifying a UE.

E//: the LS that had the list was S2-184510

after offline

Orange: if IEs are sent to home network first, what is the benefit of sending them in the initial NAS message, rather then sending them after NAS security context is set up

QC: 4G - 5G interworking

DCM: need to understand what is the difference between public key and minimal initial NAS message

DCM: keep the public key part offline

CMCC: how it is happening when USIM does the calculation

QC: with USIM calculation, other parameters need to be bound and can#t be precalculated

show of hands

In case there is no 5G security context, do you support home network public key based solution for R15?

support: Sony, Huawei, Intel, T-Mobile US 4

do not support: Nokia, Samsung, QC, CMCC, BT, Orange, E//, ZTE 8

more offline required

after offline discussion

Huawei: for R15, agree on minimal initial NAS message, but revisit protection of whole message in R16

ATT: support PKI in R16

E//: in general or for initial NAS

ATT: for now, for initial NAS, but also in general

went offline for discussion of IEs

E//: IEs can be taken from SA2 LS, principles of solution and TAU for interRAT mobility need to be decided until next meeting, maybe with conf calls

ATT: other WGs need to proceed in parallel

QC: need to get CT1 going, thus agree on flows, afterwards agree on flows.

E//: if the list of IEs includes NSSAI, then it has impact on flows as well

QC: flows could be in clause 6.4.6, base discussion on 3048 with all changes removed

continue discussion on 3048

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

**S3-183042 Discussion of intial NAS message ciphering protection**

 *Type: discussion For: (not specified)
 33.501 v..
 Source: China Mobile*

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

**S3-183043 CR of update for all encryption for initial NAS message**

 *Type: draftCR For: (not specified)
 33.501 v15.2.0
 Source: China Mobile*

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

**S3-183046 Discussion on Protection of initial NAS message**

 *Type: discussion For: (not specified)
 33.501 v..
 Source: Huawei, Hisilicon*

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

**S3-183047 Analysing the impact of the plenary decision on the proposal for initial NAS security**

 *Type: discussion For: Endorsement
 Source: Qualcomm Incorporated*

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

**S3-183048 Correcting the description of the initial NAS protection method**

 *Type: draftCR For: Approval
 33.501 v15.2.0
 Source: Qualcomm Incorporated*

**Discussion:**

QC presents

together with 3042

continued discussion on cleartext Ies

QC: NSSAI and last visited TAI need to be discussed together, ask SA2 whether that is true that it is of no value to have only one in the clear

DCM: NSSAI in clear sending is optimization of network, maybe that can be network option whether to send

Nokia: there is RAN discussion to not send NSSAI

QC: NSSAI is not only optimization, but also registration of interest

E//: in E// view, NSSAI is not privacy sensitive and can be sent in clear

BT: NSSAI can be privacy sensitive, like for company specific slices, that unencrypted is a risk

ATT: from security perspective, should be encrypted

Orange: only issue if not many customers on the slice, maybe first provision eMBB and then redirect to specific slice

BT: workaround would be helpful. but anything special for small subset will make them stand out.

QC: 3. questions: what happens if never in clear, what if NSSAI is only in clear after network securely confirms, what if only in clear on RRC

Huawei: need to go in clear

QC: only open NSSAI and last visited TAI

get number to document agreements: 3065 agreements on initial NAS security, type other

number for LS: 3066

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

**S3-183051 A way forward for the initial NAS protection mechanism**

 *Type: discussion For: Approval
 33.501 v..
 Source: Ericsson*

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

**S3-183052 Backward compaitibility mechanism for the partial ciphering feature**

 *Type: other For: Approval
 33.501 v..
 Source: Ericsson*

**Decision:** The document was **revised to S3-183053**.

**S3-183053 Backward compaitibility mechanism for the partial ciphering feature**

 *Type: other For: Approval
 33.501 v..
 Source: Ericsson*

(Replaces S3-183052)

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

**S3-183065 agreements on initial NAS message security**

 *Type: other For: Information
 Source: Qualcomm*

**Discussion:**

QC presents draft

made a permanent tdoc for reference purposes.

this document was used as basis in the evening session, see 3174 for output

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

**S3-183178 Adjusting the description of of the initial NAS protection method**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Qualcomm*

**Discussion:**

QC presents draft

E//: ed note: revisit this to deal with feedback on mobility and failure cases

ZTE, CMCC input is merged

approved

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

**S3-183174 Output of evening session on initial NAS security**

 *Type: other For: Information
 Source: NTT-Docomo*

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

#### 4.1.6 Security context

**S3-182828 Corrections to definition of 5G NAS security context**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: CATT*

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

**S3-182918 Clafirication for ngKSI**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

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

#### 4.1.7 Visibility and Configurability

#### 4.1.8 Primary authentication

**S3-182827 Correction to Nudm\_UEAuthentication\_ResultConfirmation service**

 *Type: CR For: Agreement
 33.501 v15.1.0
 Source: CATT*

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

**S3-182886 Correction to Nudm\_UEAuthentication\_ResultConfirmation service**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: CATT*

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

**S3-182951 Correction to 5G AKA procedure - no need for "SUPI or SUCI"**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Orange*

**Abstract:**

The AMF does not need to send "SUPI or SUCI" in the second message sent to the AUSF.

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

**S3-182968 Reference correction**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

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

**S3-182989 Discussion on proposal for draft CR on option to derive partial context**

 *Type: discussion For: Discussion
 Source: Qualcomm Incorporated*

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

**S3-182990 Acknowledging possibility of early calculation of EMSK**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Qualcomm Incorporated*

**Discussion:**

QC presents

Nokia: not call this partial partial security context, but it is temporary context

QC: agree

E//: Note 6:why necessary

QC: misalignment, needs to be fixed in CT1

Huawei: merge with 918

E//: SA3 should align with CT1

only note is for discussion offline

**Decision:** The document was **revised to S3-183076**.

**S3-183076 Acknowledging possibility of early calculation of EMSK**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Qualcomm Incorporated*

(Replaces S3-182990)

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

**S3-183035 Update of EAP-AKA’ RFC 5448 in progress**

 *Type: other For: (not specified)
 33.501 v..
 Source: Ericsson*

**Discussion:**

This was presented for information to SA3 that the EAP AKA' RFC is being updated and comments are requested.

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

**S3-183039 Update of EAP-AKA’ reference to make it compatible with 5G**

 *Type: other For: Approval
 33.501 v..
 Source: Ericsson*

**Discussion:**

Vdf: What is the timeline on getting this published. Ericsson: It will takes a a month or two to go through the IETF process until it is technically stable. Vdf: Maybe postpone the document until we know the status. ATT: CT1 add references to drafts all the time. QC: Is that true of replacement RFCs. ATT: Could add a note after reference. QC & NCSC both cautious about fully replacing the stabel RFC with draft at this stage. Huawei: Not sure about adding before Rel-16. Vdf: can we delete things from our specification with updtaed RFC. Ericsson: not sure yet. Juniper: References to drafts ar usde all the time. ATT: Follow CT1 process. Orange: Would like to postpone until discussed with IETF colleagues. DCM: Can we have references to both documents. Huawei: Are there changes to our specifications from the new RFC. Ericsson: Not that they are aware, but that is why are asking for review. Revised to S3-183100.

**Decision:** The document was **revised to S3-183100**.

**S3-183100 Update of EAP-AKA’ reference to make it compatible with 5G**

 *Type: other For: Approval
 33.501 v..
 Source: Ericsson*

(Replaces S3-183039)

**Discussion:**

E// presents draft

Huawei: if RFC is not ready by December?

ATT: normal process in CT to update

Todor: repeat to be superseded

Huawei: wait for next meeting to do this updated

offline again

Huawei: agreed to postpone until November

DCM: note and bring proper CR with this text

noted

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

#### 4.1.9 Secondary authentication

#### 4.1.10 Interworking

**S3-182826 Alignment of AS layer handling of EPS to 5GS handover with N2 handover**

 *Type: CR For: Agreement
 33.501 v15.1.0
 Source: CATT*

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

**S3-182885 Alignment of AS layer handling of EPS to 5GS handover with N2 handover**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: CATT*

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

**S3-182893 correction on the mobility from 5G to 4G**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: EPS algorithms in first line in step 7. Reference to TS 33.401. Vdf: Step 7, algorithm change sentence is confusing. DCM: Suggested to just reference to TS 33.401 - this will be checked offline - revised in S3-183101.

**Decision:** The document was **revised to S3-183101**.

**S3-183101 correction on the mobility from 5G to 4G**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

(Replaces S3-182893)

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

**S3-182900 Clarification on handover from EPS to 5GS**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

QC: sounds like separate IE, they come from NAS container, rewording required

Nokia: do we need the change?

Revised to 3102, kept open

**Decision:** The document was **revised to S3-183102**.

**S3-183102 Clarification on handover from EPS to 5GS**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

(Replaces S3-182900)

**Discussion:**

Huawei presents draft

keep open

QC: step 7, should be target to source container, not NAS container.

E//: ok because of reference to step 6

QC: check and then come with a separate CR for next meeting.

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

**S3-182921 Editorial corrections on the 5GS to EPS handover procedure**

 *Type: CR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

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

**S3-182922 Clarification for Target to Source container**

 *Type: CR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

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

**S3-182933 Editorial corrections on the 5GS to EPS handover procedure**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

**Discussion:**

QC: new text should be below the text on bottom

Huawei: step 9 should be indented

Nokia: what happened to requirement in step 10

DCM: make second sentence of step 10 in active voice

Nokia: should be in requirements section

E//: not a requirement

revised to 3103, kept open

**Decision:** The document was **revised to S3-183103**.

**S3-183103 Editorial corrections on the 5GS to EPS handover procedure**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

(Replaces S3-182933)

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

**S3-182934 Clarification for Target to Source container**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

**Discussion:**

E//: sounds like a new requirement, but is legacy behaviour, take wording offline.

DCM: remove shall

QC: remove text in parenthesis

Huawei: there are more shalls in unchanged text

E//: reword those as well

revised to 3104, kept open

**Decision:** The document was **revised to S3-183104**.

**S3-183104 Clarification for Target to Source container**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

(Replaces S3-182934)

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

**S3-183033 Inteworking - reply LS on key update**

 *Type: LS out For: Approval
 to RAN2
 Source: Ericsson*

**Abstract:**

This draft reply LS replies to R2-1813403 on key update.

**Discussion:**

E// presents

Huawei: NCC not send in normal case

E//: yes, not required, but protocol design is simpler.

DCM: change is not used to shall not be used

QC: there are CRs on this

2885, 3034

QC: give sentence that this is agreed, but only draft CR for organizational purposes

**Decision:** The document was **revised to S3-183071**.

**S3-183071 Inteworking - reply LS on key update**

 *Type: LS out For: Approval
 to RAN2
 Source: Ericsson*

(Replaces S3-183033)

**Discussion:**

E// presents draft

some editorials

approved

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

Attachments to this outgoing LS: S3-183070

**S3-183034 Interworking - correcting keying material in HO request message (EPS to 5GS)**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

This CR resolves EN in Clluse 8.4.2 and aligns interworking with N2-handover

**Discussion:**

E// presents

Merge with 885, but use this as baseline, because step three changes should be included with step 5.

Nokia: first KgNB is called temporary KgNB?

E//: yes

CMCC: new security context indicator, what does it mean

Huawei: should be NAS security indicator

**Decision:** The document was **revised to S3-183070**.

**S3-183070 Interworking - correcting keying material in HO request message (EPS to 5GS)**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

(Replaces S3-183034)

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

#### 4.1.11 non-3GPP access

**S3-182841 CR on Clarifictaions to Untrusted non-3GPP access clause**

 *Type: CR For: Approval
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Corrects link id# for non3GPP access, remove existing IPsec if already one exists while establishing a new one.

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

**S3-182927 Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access**

 *Type: CR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

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

**S3-182935 Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

Nokia: need clarification for same AMF

E//: don't understand that NAS count increased by one after successful authentication, should be removed

QC: corresponding NAS counts, both uplink or downlink

Huawei: ok

E//: shall be set to 0, NAS counts could have been created earlier,

QC: count set to 0 for calculation only, how does it correspond with last sentece in 7.

keep open

**Decision:** The document was **revised to S3-183119**.

**S3-183119 Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, HiSilicon*

(Replaces S3-182935)

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

**S3-183015 Draft\_CR Corrections to Untrusted Non3GPP access clause**

 *Type: other For: Approval
 33.501 v..
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

E//: ok in general, but order of execution should be make before break

Nokia: service is not continued anyways

E//: existing user plane might exist in case it is for synchronizing to new security context. Need to update for that case.

QC: agree with changes further up, context modification needs to be revisited next time

DCM: come back to next meeting with this

**Decision:** The document was **revised to S3-183120**.

**S3-183120 Draft\_CR Corrections to Untrusted Non3GPP access clause**

 *Type: other For: Approval
 33.501 v..
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-183015)

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

#### 4.1.12 NDS

**S3-182822 Update NDS/IP scope with application layer crypto profiles**

 *Type: draftCR For: Approval
 33.210 v15.0.0
 Source: Juniper Networks, Ericsson*

**Abstract:**

Changes corresponding to release 15, including the differences in TLS are made for release 16.

**Discussion:**

Juniper presents

QC: give hint for MCC to have same reference numbers

DCM: normative words in Note

E//: fix later and synchronize with R15

action on Steve and Christine to align other SA3 specs.

revised to 3122

**Decision:** The document was **revised to S3-183122**.

**S3-183122 Update NDS/IP scope with application layer crypto profiles**

 *Type: draftCR For: Approval
 33.210 v15.0.0
 Source: Juniper Networks, Ericsson*

(Replaces S3-182822)

**Discussion:**

Juniper presents draft

QC: replace doc number with CR number in final revision for next meeting

approved

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

**S3-182824 Update references**

 *Type: draftCR For: Approval
 33.210 v15.0.0
 Source: Juniper Networks, Ericsson*

**Abstract:**

Missing and incorrect references.

**Discussion:**

Juniper presents

NCSC: for R15 or 16

Juniper: for 15

NCSC: cover sheet wrong

revised to 3121

**Decision:** The document was **revised to S3-183121**.

**S3-183121 Update references**

 *Type: draftCR For: Approval
 33.210 v15.0.0
 Source: Juniper Networks, Ericsson*

(Replaces S3-182824)

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

**S3-182825 Move TLS crypto profiles to TS 33.210**

 *Type: draftCR For: Approval
 33.310 v16.0.0
 Source: Juniper Networks, Ericsson*

**Discussion:**

Juniper presents

VF: delete Void because there is text in there

approved

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

#### 4.1.13 Service based architecture

##### 4.1.13.1 Interconnect (SEPP related)

**S3-182820 Preference of protection policies on the N32 interface**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Deutsche Telekom AG*

**Abstract:**

Preference of provisioned and dynamically exchanged protection policies is not defined.

New clause 13.2.z.6 is added to define preference.

**Discussion:**

DCM: what happens to policies of lower precedence

Subclause in 1. need to be revised.

BT and Vdf had concerns with how you could move away from manually configurable override policy – this is taken offline.

Ericsson: Need to clarify what type of policy. Granularitly of policy needs to be clarified.

CMCC: Questioned whether the policy precedence is really needed.

Juniper: Thinks that the policy precedence can be simplified overall.

Revised to S3-183083 and kept open

**Decision:** The document was **revised to S3-183083**.

**S3-183083 Preference of protection policies on the N32 interface**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Deutsche Telekom AG*

(Replaces S3-182820)

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

**S3-182821 Handling of encrypted IEs on the N32 interface**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Deutsche Telekom AG*

**Abstract:**

Existing text on default behaviour of encrypted IEs in the SEPP is misleading.

Rephrased and moved a paragraph from clause 13.2.z.4 to clause 13.2.a.1.

**Discussion:**

Vdf: Last sentence is not clear – this sentence will re-worded -> revised to

S3-183082 – kept open for editorial revisions

**Decision:** The document was **revised to S3-183082**.

**S3-183082 Handling of encrypted IEs on the N32 interface**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Deutsche Telekom AG*

(Replaces S3-182821)

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

**S3-182823 Removal of Editor’s Note on security on the N32 interface**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Deutsche Telekom AG*

**Abstract:**

Editor’s Note was already implemented. Details on the use of a PKI are out of scope and will be addressed in GSMA DESS.

**Discussion:**

Same change as S3-182987.

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

**S3-182974 Clarification to N32 Procedure on insertion of decrypted values**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Discussion:**

Nokia: Is Note 1 needed – this was agreed

Vdf: First sentence and second sentence are mutually exclusive and first is not needed as it is a negative.

First sentence will be reword to make it ‘shall ignore’ and moved to after second sentence (which has instead removed). Revised to S3-183085 and kept open.

**Decision:** The document was **revised to S3-183085**.

**S3-183085 Clarification to N32 Procedure on insertion of decrypted values**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

(Replaces S3-182974)

**Discussion:**

E// presents draft

E// proposing to remove the references in the cleartext encapsulation block

kept open

E// suggest to note

noted

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

**S3-182975 Length of IV salt and sequence counter**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

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

**S3-182981 PLMN ID protection in N32 message**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

DT: Assume that PLMN is checked at N32 setup – prevents the need of receiving message on N32-f and validate PLMN there.

Huawei: Prevent an authorized network for claiming to be another network.

DT: Is the threat that one roaming partner is impersonating another one.

Huawei: Yes.

The document was kept open as the problem is not being fully agreed at this time.

Noted

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

**S3-182987 Remove EN in 13.2**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

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

**S3-182988 Clarifications to clause 13.2.x**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Clarifications in SBA clause 13.2.x

**Discussion:**

Ericsson had editorials that will be dealt with -> revised to S3-183078 – kept open

**Decision:** The document was **revised to S3-183078**.

**S3-183078 Clarifications to clause 13.2.x**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182988)

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

**S3-182996 Remove EN in clause 13.2.y.1**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Remove EN in clause 13.2.y.1

**Discussion:**

Vdf: Correction of context to Context in step c,

NCSC: reference xx becomes zz, change to first line

BT: Delete between NFs-> kept open for editorials –> revised to S3-183079 - kept open

**Decision:** The document was **revised to S3-183079**.

**S3-183079 Remove EN in clause 13.2.y.1**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182996)

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

**S3-182998 Correction in step 2 of 13.2.y.2**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Correction in step 2 of 13.2.y.2

**Discussion:**

NCSC: A.1 is added to a subclause reference – agreed.

NCSC: should it be Application Layer Security rather than application layer security to make in clear that it is actually something – this was agreed in general and will be fixed in this document -> revised to S3-183080 – kept open

**Decision:** The document was **revised to S3-183080**.

**S3-183080 Correction in step 2 of 13.2.y.2**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182998)

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

**S3-182999 Corrections in 13.2.y.4 on N32-f context ID**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Corrections in 13.2.y.4 on N32-f context ID

**Discussion:**

NCSC: 3rd paragraph remove .1 from subclause -> approved as S3-183081

**Decision:** The document was **revised to S3-183081**.

**S3-183081 Corrections in 13.2.y.4 on N32-f context ID**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182999)

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

**S3-183001 Clarifications and corrections in clause 13.2.a**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Clarifications and corrections in 13.2.a

**Discussion:**

NCSC: Encapsulated maybe should become encapsulation – needs a consistency check

Went offline for more checks

**Decision:** The document was **revised to S3-183127**.

**S3-183127 Clarifications and corrections in clause 13.2.a**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-183001)

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

**S3-183002 pCR to S3-182700 regarding N32-f key hierarchy**

 *Type: other For: (not specified)
 33.501 v..
 Source: China Mobile*

**Discussion:**

Ericsson: rewording the first sentence rather than removing to clarify the number of keys and salts used in a connection -> taken offline for rewording and revised as S3-183084.

**Decision:** The document was **revised to S3-183084**.

**S3-183084 pCR to S3-182700 regarding N32-f key hierarchy**

 *Type: other For: -
 33.501 v..
 Source: China Mobile*

(Replaces S3-183002)

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

**S3-183003 N32 related definitions**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

N32 related definitions

**Discussion:**

Ericsson proposal on N32 transaction definition being added

Vdf: Wants normative text removed from defintions.

Juniper: Some concerns that will be taken offline.

Revised to S3-183086 and taken offline.

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

**S3-183086 N32 related definitions**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

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

**S3-183009 Security aspects of SEPP - IPX communication**

 *Type: discussion For: (not specified)
 33.501 v..
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Discussion paper on SEPP to IPX communication including routing aspects

**Discussion:**

Nokia presents

VF: each operator has their own preference, so it is only a Note that the communication will have to be confidentiality protected.

Agreed not to standardize one option

agreed to send an LS to CT4

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

**S3-183044 comments on Handling of encrypted IEs on the N32 interface**

 *Type: draftCR For: Approval
 33.501 v15.2.0
 Source: NTT DOCOMO*

**Abstract:**

Existing text on default behaviour of encrypted IEs in the SEPP is misleading.

Rephrased and moved a paragraph from clause 13.2.z.4 to clause 13.2.a.1.

**Discussion:**

Wants to keep text that was deleted in the above document and to more fully explain the text in another place.

The proposal changes were agreed and it was merged in S3-183082

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

**S3-183064 LS Inter-PLMN security**

 *Type: LS out For: Approval
 to CT4
 Source: Nokia*

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

##### 4.1.13.2 Other

**S3-182901 Editorial corrections on Authorization of NF service access**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Nokia: Change of NF instance Id sentence is not correct – this was reverted to original – approved as S3-183087

**Decision:** The document was **revised to S3-183087**.

**S3-183087 Editorial corrections on Authorization of NF service access**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

(Replaces S3-182901)

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

**S3-182902 Handling for the service access failure**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Vdf: Reword if verification is failed to if verification fails.

DT: Thinks the changes are unnecessary.

CMCC: Agrees with DT on one change.

Nokia: did not agree to changes.

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

**S3-182903 Delete EN in SBA Requirements**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

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

**S3-182904 Topology hiding for SBA**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: Not in favour because NRF is not only entiy doing topology hiding

DT: Do not support the changes as there is no clear idea of Topology hiding entity.

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

**S3-182905 Add discover procedure as a pre-requisite for obtaining access token**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Ericsson: First change is not correct as discovery is not mandatory

Huawei: Discovery is needed in normal case

Nokia: Original intention was to mandate discovery but it is better to not include first changes as there.

Only second change is agreed -> Approved as S3-183088.

**Decision:** The document was **revised to S3-183088**.

**S3-183088 Add discover procedure as a pre-requisite for obtaining access token**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

(Replaces S3-182905)

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

**S3-182906 Clarifications on AccessToken\_Get Response message**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

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

**S3-182985 Token caching**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Discussion:**

Huawei/Nokia: suggest clarification that tokens should only be used for intended purpose

Vdf: wanted some rewording of the sentence

Revised to S3-183089 - kept open

**Decision:** The document was **revised to S3-183089**.

**S3-183089 Token caching**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

(Replaces S3-182985)

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

**S3-182986 NF instances in token claims**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Discussion:**

Nokia: just add ‘(s)’ rather than an ‘or ..’ and same change higher up.

Approved as S3-183090

**Decision:** The document was **revised to S3-183090**.

**S3-183090 NF instances in token claims**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

(Replaces S3-182986)

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

#### 4.1.14 Privacy

**S3-182862 NF discovery with SUCI**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: NEC Corporation*

**Abstract:**

This draft CR clarifies the UDM/AUSF discovery using Routing ID along with the Group ID.

**Discussion:**

NEC presents

Orange: this should be SA2 or CT4

E//, Huawei: agree

NEC: send LS to SA2 including this

Orange: provide as company contribution to SA2

noted

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

**S3-182967 Removing mandatory text from note**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

Orange: make this normative

E//: clarify that default value is specified in 23.003

Orange: cross-reference that note is not used

E//: 23.003 defines normative behavior

BT: how is the identifier set back after an unauth emergency call

VF: do we need to say anything about SIM

Nokia: come next meeting with proposal

approved

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

**S3-182976 Privacy - max. size of scheme-output for proprietary protection schemes**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

This contribution proposes maximum size of scheme-output for proprietary SUPI concealment schemes.

**Discussion:**

E// presents

NCSC: very tight boundary, increase to 1024

VF: 256bit study will need larger sizes

DCM: without point compression you already need larger than 1024

CMCC: no security reason to limit size

E//: maximum size required, also maximum size of message that can transport this

NCSC: need a note on size limit

BT: reason to defend against DoS attack

VF: only make this for guidance

QC: need normative text

Offline discussion

revised to 3123

**Decision:** The document was **revised to S3-183123**.

**S3-183123 Privacy - max. size of scheme-output for proprietary protection schemes**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

(Replaces S3-182976)

**Discussion:**

E// proposes to send an LS and tell current status of understanding, difficult to give good estimate.

Keep open for now

noted

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

**S3-182977 Privacy - LS on maximum output size of SUPI concealment schemes**

 *Type: LS out For: Approval
 to CT1, CT4, cc RAN2, SA2
 Source: Ericsson*

**Abstract:**

This LS informs CT1/CT4 about the maximum size of scheme-output for proprietary SUPI concealment schemes.

**Decision:** The document was **revised to S3-183142**.

**S3-183142 Privacy - LS on maximum output size of SUPI concealment schemes**

 *Type: LS out For: Approval
 to CT1, CT4, cc RAN2, SA2
 Source: Ericsson*

(Replaces S3-182977)

**Discussion:**

E// presents draft

Orange: what is the purpose of the LS?

E//: give guidance to CT then update the TS later

QC: ask CT for maximum size and send approved CR

Orange: for time being not update CR

kept open

VF: plus size of output

NCSC: size at least 100.000bytes

QC: reformulate question for clarity: what is the size limit

taken offline

agreed

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

#### 4.1.15 Incoming and outgoing Lses

**S3-182809 LS on Transmission mechanism of SUCI in NAS procedure**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: C1-185663*

**Decision:** The document was **replied to in S3-183073**.

**S3-183073 Reply to: LS on Transmission mechanism of SUCI in NAS procedure**

 *Type: LS out For: approval
 to CT1
 Source: NEC*

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

**S3-182810 LS on Clarifications on SUPI definition and NAI format**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: C4-186573*

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

**S3-182811 Reply LS on AUSF/UDM instance selection and SUCI parameters**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: C4-186606*

**Discussion:**

Nokia presents

Nokia: SUPI type is missing from SA3 spec, added in 2954,

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

**S3-182812 LS on Key Update**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: R2-1813403*

**Discussion:**

DCM presents

Huawei: NCC doesn't need to be sent

E//: response proposal in 3033

**Decision:** The document was **replied to**.

**S3-182813 LS on Routing ID**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: S2-188870*

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

**S3-182814 Reply to CT4 LS on Nausf\_SoRProtection service**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: S2-189035*

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

**S3-182817 LS on devices behind 5G-RG accessing the 5GC**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: S3i180377*

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

**S3-182818 LS on SG17 work item X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: ITU-T SG17*

**Discussion:**

Colin presents

NCSC: Propose to send back TR on 256 bit from after Spokane.

NCSC: what is this covering that is not covered in ETSI or 3GPP

CMCC: not only symmetric, but also asymmetric.

VF: seems a complete copy of 256 study. Seems like straight duplication.

Chair: give message that this is duplicating work.

VF: ITU could have focussed on ITU based standards, or radio

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

**S3-182819 Reply LS on Routing ID**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: CP-182238*

**Discussion:**

Nokia presents

QC: comment, routing identifier is only one parameter, other things like public key and ist identifier may also change, so solution needs to update other parameters as well

VF: like with SoR: there is a secure mechanism with OTA over many bearers, just an excuse for yet another mechanism for updating the USIM. So update the OTA specifications.

E//: which group is responsible for deciding whihc mechanism

VF: security requirements CIA all provided by OTA mechanism

QC: what is the confidentiality risk

VF: there are other fields like management information that shouldn't be in clear. OTA is protected for all of the route

Orange: what do we need to update, only routing ID, or also other parameters

Nokia: LS is only about routing ID

QC: SIDF is part of UDM, so there may be a different private key.

together with 888, 3049

**Decision:** The document was **replied to in S3-183074**.

**S3-183074 Reply to: Reply LS on Routing ID**

 *Type: LS out For: approval
 to CT1, SA2,CT, cc CT4, CT6
 Source: BT*

**Discussion:**

This contribution will need an offline discussion.

Content: endpoint, confidentiality, integrity, replay protection, 4G or 5G

VF presents draft v2 to understand the status

Orange: only QC thinks that other parameters than routing ID needs to changed

QC: If operator uses different public keys for different UDMs, then it has to be done, therefore it is may

BT: CT sent a list of parameters

VF: there was change request to SUCI parameters

Idemia: we already have a way of distributing public key, scheme identifier is provision already

Nokia: better to have generic parameter, keep note in

Gemalto: want note out

Samsung: if routing ID is corrupted - there is no chance of having it corrupted, because there is integrity protection

DCM: problem with word corruption

Nokia: confirmation can take care of this

E//: no matter what we do, there will always be some UEs not reachable and therefore not updated. what is the sentence about the breaking security of USIM

Nokia: are there sufficient number of AMF bits

VF: makes use of propietary AMF bits

QC: may not be forwad compatible

Orange: why optional confidentiality

Nokia: AMF solution not yet discussed in SA3

QC: solution not fully analysed needs to be added

Orange: make clear these are options, none of this is agreed

DCM: say that option 1 has no standards impact, but also say that there has been no further analysis

E//: remove question what requirements need to be considered that are not fulfilled by OTA.

Orange: that question was agreed

Gemalto: who will select the solution

ATT: reason why OTA is not sufficient because of number of changes (forwarded from Verizon)

DCM: ask for general requirements as well

keep open

BT chaired an evening session on this

Wording of solutions was done offline

Gemalto: v10 added sentence of storing Routing ID in ME alternatively

QC: would be an alternative

VF, Orange disagree with this solution

QC: remove reference to study.

Huawei: remove option OTA

VF: request the limitation that ruled out OTA was agreed

Orange: other privacy parameters may need to be changed should not be LS

Orange: not clear that configuration information may need confidentiality protection

VF: that was agreed

BT: in the offline discussion stuff outside of the options was agreed

Gemalto: support confidentiality protection

QC, Samsung: ok with Orange position

Apple, ZTE: with VF

Orange: remove OTA is included for reference

E//: why does the user lose service if USIM is moved to different UE

QC: reference removed, so delete

DCM what is the work item for this

QC: 5G phase 1 sec

E//: do we need all groups?

BT: full action to SA2 and CT1

Apple: SA3 requires that ... break security of USIM, that is for SA3 not other groups

E//: all options do this? Can't have excluded options in LS

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

**S3-182842 Discussion on LS S3-182809 timer on transmission of SUCI.**

 *Type: discussion For: Discussion
 33.501 v..
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

together with 937 and 941

E//: Nokia it is possible to retrnasmit the SUCI?

Nokia: two types of errors: local error between UE and AMF, authentication error between UE and UDM

E/: UE doesn't know, it may not get the cause, UE can retransmit independent of error.

QC: if part of same registration procedure.

Nokia: CT1 question relevant to GMM clause, so only simple retransmission

QC: ok to retransmit if part of same registration procedure

NEC: regardless of failure scenario it can be retransmitted.

VF: where is threat with 100sec time window coming from? why 100sec?

NEC: this is not the lifetime, but it reflects the solution

VF: relevant for chosing solution

NEC: gives wrong impression, should be secure for longer

VF: needs to be minuted that cons in 937 in solution 2 that freshness not maintained for 100s is incorrect.

group agrees

chair: agreement for QC sentence in LS.

Nokia: reservations

on CR: QC, E// sentence not required

on LS

Taka: UE can send the same SUCI for all kind of errors

E//: prefer QC proposal

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

**S3-182884 Guidance on initial NAS message protection**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: SP-180914*

**Discussion:**

Chair presents

Orange: says to reduce information sent in clear.

Move to NAS security.

**Decision:** The document was **replied to in S3-183066**.

**S3-183066 LS on initial NAS security agreements**

 *Type: LS out For: approval
 to SA, SA2, CT1, RAN2, RAN3
 Source: Qualcomm*

**Discussion:**

QC presents

E//: prefer to remove stage 3 IEs

DCM: prefer to keep for precision

Orange, Nokia: agree

Nokia: ciphered means: the implication of the above

E//: need more time

offline

E//: ok

attach 3178

approved

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

Attachments to this outgoing LS: S3-183178

**S3-183050 Discussion on LS on Routing ID Update**

 *Type: discussion For: Endorsement
 Source: Nokia, Nokia Shangahi Bell*

**Discussion:**

Nokia presents

VF: strongly object to SoR mechanism, as it is unnessessary, impractical, RI becomes ME editable

Huawei: support for Huawei documents 2888 and 2919 from Verizon, add as Verizon cosigner in revision.

Huawei: OTA not practical from SA2 point of view

Orange: object to SoR mechanism, there are simpler mechanisms

ATT: agrees with Verizon, support solution in R15

VF: RI becomes ME editable file

Orange: need something much simpler, ask for more time to consider a solution

BT: integrity on routing ID is that one could desynchronize USIM for denial of service, security required UICC to UDM.

Samsung: support Huawei proposal, if the UE does something with RI, it can do after reading it

Idemia: end to end is between UICC and home network needs to be clarified. RI can be in format of domain name, then the network can resolve the RI and move to correct IP address

DCM: problem that it is only during registration, only move subscriber after successful registration

BT: for SoR is only partly in registration, OTA stays as option, here, UDM relocation is only in registration

VF: more often USIM is moved between handsets, while most subscribers never move between UDMs

Gemalto: endpoint shall be UICC.

E//: even with such a mechanism, there will be USIMs with wrong routing IDs, so that kind of mechanism is required anyways

Orange: OTA exists already, unclear what SA2 wants to achieve, requirements should be requested in an LS.

DT: support sending LS

E//: state some security requirements at least.

Alex will write response to 819

Orange: not include security requirements, in order to agree

E//: sec requirements were asked for in LS

VF: scope needs to be defined in offline

DCM: try to agree on security requirements, and request SA2 requirements

Gemalto: security requirements only after we have response from SA2

BT: start with two parts: security requirements + question on what's wrong with OTA

Orange: need to understand what effective means.

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

**S3-183164 Reply LS on Clarifications on SUPI definition and NAI format**

 *Type: LS out For: Approval
 to -
 Source: IDEMIA*

**Discussion:**

Idemia presents draft

QC: don't need this LS, wait for SA2 LS if used for other types of SUPI.

Idemia: if SUPI type is not needed in R15, then remove from our specification

VF: how are we going to inform CT4

Nokia: there was no question in LS

Gemalto: but it is in our spec

QC: revisit this after SA2 reply

kept open

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

#### 4.1.16 Others

**S3-182829 Corrections to references for security related service in clause 14**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: CATT*

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

**S3-182845 Discussion on fast re-authentication**

 *Type: discussion For: Endorsement
 Source: ZTE Corporation, China Mobile, China Unicom*

**Discussion:**

ZTE presents

chair: no discussion on new SIDS here, just a few comments

Orange: not against fast reauth, but no explicit study on this

Nokia: discussion in Belgrade already, but decided against

Orange: agree, only as specific key issue

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

**S3-182888 Discussion on the RI update requirement**

 *Type: discussion For: Endorsement
 33.501 v..
 Source: Huawei, Hisilicon*

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

**S3-182919 Solution for RI update mechanism**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: why is this better than SIM OTA

VF: same comment

BT: new mechanisms introduced all the time

DCM: is this required in R15, or can it be in R16

Nokia: it was in CT plenary because it was desired in R15

together with 3050

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

**S3-182920 Editorial corrections on SoR**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Samsung: already implemented

noted

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

**S3-182929 Editorial changes to the 5G AV definition**

 *Type: draftCR For: Agreement
 33.501 v15.1.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Nokia: already implemented in last version

noted

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

**S3-182942 Achieving higher data rates for UP IP**

 *Type: discussion For: Endorsement
 Source: Motorola Mobility, Lenovo*

**Abstract:**

This paper discusses the possibility on achieving higher data rates for user plane integrity protection, taking the current limitations into account.

**Discussion:**

Lenovo presents

DT: is this related to VFs SID proposal

Lenovo: this is for 5G, VFs is for 4G

Apple: support this

CMCC: unclear which part is included in partial integrity protected

Nokia: if there is a mismatch what are you supposed to do, discard whole PDU? What is the window?

QC: don't make this more complicated, instead focus on developng max rate integrity.

Noted

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

**S3-182954 Corrections and additions in definitions and related clauses**

 *Type: draftCR For: (not specified)
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

Colin: CT4 gives more information away

VF:on CT4 changes increasingly hard to find out how this is formatted, coding is unclear, useless as specification

Idemia: need to describe how SUCI type is selected

QC: there is confusion between SUCI types and SUPI format and NAI format. Needs further work, clarify when SUPI and SUCI are in that format

Orange: shouldn't this be SA2 discussion, Nokia CR is just aligning, format is between SA2 and CT4

ATT: remind of timing of meetings, need ot respond sooner than later.

Nokia: put editor's note.

E//: maybe this is using the wrong baseline

QC: what are the other types of identifiers

BT: this indicator not sent in clear, not routing related

remove the example

DCM: definition needs to reworded

QC: no definition, just put as reference in text

E//: there are editorials other than alignment

**Decision:** The document was **revised to S3-183072**.

**S3-183072 Corrections and additions in definitions and related clauses**

 *Type: draftCR For: -
 33.501 v15.1.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182954)

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

**S3-182957 Adding reference to 33.501 in 33.102**

 *Type: draftCR For: (not specified)
 33.102 v15.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

no comments

approved

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

**S3-183017 Correction to the Security Service for Steering of Roaming**

 *Type: draftCR For: Approval
 33.501 v15.1.0
 Source: Ericsson*

**Abstract:**

Missing input in the Steering of Roaming service definition and changes in the logic to simplify AUSF handlings.

**Discussion:**

E// presents

VF: is this aligned with CT?

E//: unrelated

VF: if operator doesn't use SoR, does it still work?

Samsung: it is all in the home network

approved

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

**S3-183036 Work on improving perfect forward secrecy in 5G network access**

 *Type: other For: (not specified)
 Source: Ericsson*

**Discussion:**

E// presents

Orange: should be on detection, not on per connection.

VF: related to LTKUP, which VF wants to move forward to implementation, not necessary to do PFS for every transaction, more periodic

noted

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

**S3-183037 Using EAP-TLS with TLS 1.3**

 *Type: other For: (not specified)
 Source: Ericsson*

**Discussion:**

E// presents

Orange: this is not standardized in 33.501, but informative in 33.501

noted

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

**S3-183049 Nokia comments to S3-182888**

 *Type: discussion For: Endorsement
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

VF: replay attacks need to be considered again for this solution

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

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

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

**S3-182868 Integrity protection of RRC-signalling**

 *Type: pCR For: (not specified)
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to Integrity protection of RRC-signalling

**Discussion:**

Ericsson: Think the test has limited value as it is more like protocol testing than local hardening. Nokia: This sort of test is covered in an existing case. NEC: This special behavior for gNB. Nokia: The protection of standardized interface will be covered by inter-operability testing. Huawei: Can capture this requirement as in option 2 – this was agreed -> Revised to S3-18307

**Decision:** The document was **revised to S3-183107**.

**S3-183107 Integrity protection of RRC-signalling**

 *Type: pCR For: -
 33.511 v0.1.0
 Source: NEC Corporation*

(Replaces S3-182868)

**Discussion:**

NEC presents draft

other revisions with same issue are approved as well

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

**S3-182865 Integrity protection of user data between the UE and the gNB**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to integrity protection of user data between the UE and the gNB

**Discussion:**

Capture this requirement as in option 2 – this was agreed – revised to S3-183108

**Decision:** The document was **revised to S3-183108**.

**S3-183108 Integrity protection of user data between the UE and the gNB**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

(Replaces S3-182865)

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

**S3-182834 Security Assurance Requirement and Test for AS NULL Integrity Disabling in the gNB**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This contribution proposes to add a security assurance requirement and the corresponding test case to TS 33.511 to assure AS NULL integrity algorithm is not used in the deployments where support of unauthenticated emergency session is not a regulatory req

**Discussion:**

Huawei/NEC: Deployment requirement is not appropriate for the TS. DT supported inclusion of the text as a similar case for eNB. Approved.

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

**S3-182835 Security Assurance Requirement and Test for failed Integrity Verification in the gNB**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This contribution proposes to add two security assurance requirements and the corresponding test cases to TS 33.511 to assure RRC/UP integrity check failure is correctly handled by the gNB.

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

**S3-182867 Ciphering of RRC-signalling**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to Ciphering of RRC-signalling

**Decision:** The document was **revised to S3-183109**.

**S3-183109 Ciphering of RRC-signalling**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

(Replaces S3-182867)

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

**S3-182863 Ciphering of user data between the UE and the gNB.**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to Ciphering of user data between the UE and the gNB

**Discussion:**

NEC presents

same change as in 868

**Decision:** The document was **revised to S3-183110**.

**S3-183110 Ciphering of user data between the UE and the gNB.**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

(Replaces S3-182863)

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

**S3-182866 Replay protection of user data between the UE and the gNB**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to replay protection of user data between the UE and the gNB

**Discussion:**

NEC presents

Nokia: same changes in this?

NEC: no option 1 or 2.

Nokia: only requirements, no test required, do in interoperability test

DCM: if not specified in interop test, it should be here

approved

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

**S3-182869 Replay protection of RRC-signalling**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to replay protection of RRC-signalling

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

**S3-182870 Ciphering of user data based on the security policy sent by the SMF**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to Ciphering of user data based on the security policy sent by the SMF

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

**S3-182872 Integrity protection of user data based on the security policy sent by the SMF**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to integrity protection of user data based on the security policy sent by the SMF

**Discussion:**

NEC presents

BT: is the 64kbit/s limit reflected in policy? Add test case if data rate of integrity protected traffic is exceeded

DCM: what does the gNB do if overloaded with IP traffic?

BT: not clear at all, ok, accept this as is, and fix later

approved

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

**S3-182873 Confidentiality protection on the gNB DU-CU F1-U interface for user plane**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to Confidentiality protection on the gNB DU-CU F1-U interface for user plane

**Discussion:**

NEC presents

problems with Ipsec protection implementation

noted

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

**S3-182874 Integrity protection on the gNB DU-CU F1-U interface for user plane**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to Integrity protection on the gNB DU-CU F1-U interface for user plane

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

**S3-182875 Replay protection on the gNB DU-CU F1-U interface for user plane**

 *Type: pCR For: Approval
 33.511 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add gNB security requirement and test case related to replay protection of user data sent between gNB DU-CU over F1-U interface

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

**S3-183060 Draft TS 33.511**

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

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

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

**S3-182837 Security Assurance Requirement and Test for Kseaf Handling in the SEAF/AMF**

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

**Abstract:**

This contribution proposes to add a security assurance requirement and the corresponding test case to TS 33.512 to assure correct handling of the Kseaf in the SEAF/AMF.

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

**S3-182838 Security Assurance Requirement and Test for NAS NULL Integrity Disabling in the AMF**

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

**Abstract:**

This contribution proposes to add a security assurance requirement and the corresponding test case to TS 33.512 to assure NAS NULL integrity algorithm is not used in the deployments where support of unauthenticated emergency session is not a regulatory re

**Discussion:**

Nokia presents

NEC: collides with 877, merge those

Nokia: separate issues

approved

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

**S3-182839 Security Assurance Requirement and Test for RES\* verification failure handling in the AMF**

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

**Abstract:**

This contribution proposes to add a security assurance requirement and the corresponding test case to TS 33.512 to assure correct handling by the AMF in case of RES\* verification failure during authentication and key agreement procedure.

**Discussion:**

Nokia presents

NEC: too complex to test this, a complete network is needed for test

DCM: need a test for this purpose

Nokia: come back next meeting

noted

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

**S3-182840 Security Assurance Requirement and Test for synchronization failure handling in the AMF**

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

**Abstract:**

This contribution proposes to add a security assurance requirement and the corresponding test case to TS 33.512 to assure correct handling by the AMF in case of synchronisation failure during authentication and key agreement procedure.

**Discussion:**

Nokia presents

BT: there is no more authentication vector expiration, so how is this working

DCM: this is about sync failure

NEC: precondition needs to be adapted with emulated core network

**Decision:** The document was **revised to S3-183111**.

**S3-183111 Security Assurance Requirement and Test for synchronization failure handling in the AMF**

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

(Replaces S3-182840)

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

**S3-182876 Ciphering of NAS signalling message**

 *Type: pCR For: Approval
 33.512 v0.2.0
 Source: NEC Corporation, Deutsche Telekom AG*

**Abstract:**

This contribution proposes to add AMF security requirement and test case related to confidentiality protection of NAS signalling messages

**Discussion:**

NEC presents

same option 2 comment

revised

**Decision:** The document was **revised to S3-183112**.

**S3-183112 Ciphering of NAS signalling message**

 *Type: pCR For: Approval
 33.512 v0.2.0
 Source: NEC Corporation, Deutsche Telekom AG*

(Replaces S3-182876)

**Discussion:**

NEC presents draft

Nokia: how can the tester get private key in real network? Ok in simulation network.

Approved

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

**S3-182877 Integrity protection of NAS signalling messages**

 *Type: pCR For: Approval
 33.512 v0.2.0
 Source: NEC Corporation, Deutsche Telekom AG*

**Abstract:**

This contribution proposes to add AMF security requirement and test case related to integrity protection of NAS signalling messages

**Discussion:**

NEC presents

same option 2 comment

revised

**Decision:** The document was **revised to S3-183113**.

**S3-183113 Integrity protection of NAS signalling messages**

 *Type: pCR For: Approval
 33.512 v0.2.0
 Source: NEC Corporation, Deutsche Telekom AG*

(Replaces S3-182877)

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

**S3-182878 Replay protection of NAS signalling messages**

 *Type: pCR For: Approval
 33.512 v0.2.0
 Source: NEC Corporation, Deutsche Telekom AG*

**Abstract:**

This contribution proposes to add AMF security requirement and test case related to replay protection

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

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

**S3-182879 Confidentiality protection of user data transported over N3 interface**

 *Type: pCR For: Approval
 33.513 v0.1.0
 Source: NEC Corporation, Samsung*

**Abstract:**

This contribution proposes to add UPF security requirement and test case related to confidentiality protection of user data transported over N3 interface

**Discussion:**

NEC presents

E//: same comment as before, more a protocol test, like F1

Huawei: agree

NEC: different, as feature is not mandated to be implemented

E//: requirements are ok. Does this have to be tested

NEC: the steps are removed, refer to 33.117

revised to 3114

**Decision:** The document was **revised to S3-183114**.

**S3-183114 Confidentiality protection of user data transported over N3 interface**

 *Type: pCR For: Approval
 33.513 v0.1.0
 Source: NEC Corporation, Samsung*

(Replaces S3-182879)

**Discussion:**

NEC presents draft

approved

same for 115

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

**S3-182880 Integrity protection of user data transported over N3 interface**

 *Type: pCR For: Approval
 33.513 v0.1.0
 Source: NEC Corporation, Samsung*

**Abstract:**

This contribution proposes to add UPF security requirement and test case related to integrity protection of user data transported over N3 interface

**Discussion:**

NEC presents

refer to steps in 117

revised to 3115

**Decision:** The document was **revised to S3-183115**.

**S3-183115 Integrity protection of user data transported over N3 interface**

 *Type: pCR For: Approval
 33.513 v0.1.0
 Source: NEC Corporation, Samsung*

(Replaces S3-182880)

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

**S3-182881 Replay protection of user data transported over N3 interface**

 *Type: pCR For: Approval
 33.513 v0.1.0
 Source: NEC Corporation, Samsung*

**Abstract:**

This contribution proposes to add UPF security requirement and test case related to integrity protection of user data transported over N3 interface

**Discussion:**

NEC presents

E//: same comment as 880, should have similar tests for all IPsec would be sensible,

NEC: currently nothin in 117

Huawei: really only testing that IPsec is there.

Samsung: if IPsec is implemented, then this is the test procedure

DCM: remove the test steps replace by ed note to point to 117

Huawei: not in position to test Ipsec

**Decision:** The document was **revised to S3-183116**.

**S3-183116 Replay protection of user data transported over N3 interface**

 *Type: pCR For: Approval
 33.513 v0.1.0
 Source: NEC Corporation, Samsung*

(Replaces S3-182881)

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

**S3-183062 Draft TS 33.513**

 *Type: draft TS For: Approval
 33.513 v0.2.0
 Source: Samsung*

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

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

**S3-182836 Security Assurance Requirement and Test for synchronization failure handling in the UDM**

 *Type: pCR For: Approval
 33.514 v0.1.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

This contribution proposes to add a security assurance requirement and the corresponding test case to TS 33.514 to assure correct handling by the UDM in case of synchronisation failure during authentication and key agreement procedure.

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

**S3-182882 Resolving the SUPI from the SUCI based on the protection scheme used to generate the SUCI**

 *Type: pCR For: Approval
 33.514 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add security related requirements of UDM and test case related to the de-concealment of the SUCI based on protection scheme used to generate SUCI

**Discussion:**

NEC presents

CMCC: case 1 step 1: N1 to AMF not AUSF, SA3 don't mention UDR

NEC: change to UDM?

CMCC: ok

BT: requirement to bind to registration process to SEAF rather than AMF.

DCM: title is about AMF.

NEC: typo

E//: this is like functional test.

BT: this is so critical and important, needs to be tested. Ed note: how note 3 of subclause XXX can be addressed

revised to 3117

**Decision:** The document was **revised to S3-183117**.

**S3-183117 Resolving the SUPI from the SUCI based on the protection scheme used to generate the SUCI**

 *Type: pCR For: Approval
 33.514 v0.1.0
 Source: NEC Corporation*

(Replaces S3-182882)

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

**S3-182883 Storing authentication status of UE**

 *Type: pCR For: Approval
 33.514 v0.1.0
 Source: NEC Corporation*

**Abstract:**

This contribution proposes to add security related requirements of UDM and test case related to the storing of authentication status of UE by UDM

**Decision:** The document was **revised to S3-183118**.

**S3-183118 Storing authentication status of UE**

 *Type: pCR For: Approval
 33.514 v0.1.0
 Source: NEC Corporation*

(Replaces S3-182883)

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

**S3-183063 Draft TS 33.514**

 *Type: draft TS For: Approval
 33.514 v0.2.0
 Source: NEC*

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

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

## 5 Studies

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

**S3-182890 Security procedure when returns to E-UTRAN or NR from UTRAN**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: title says to 4 or 5g, but requirements only about going back to 4G, it is shall, not should

E//: why is this relevant?

Huawei: real problem possible,

E//: this has impact on legacy 4G

BT: in scope, because if not performed then there may be impact on carriers not deploying this, based on SA plenary precondition.

VF: English needs to be fixed

DCM: network and UE shall prohibit return after SRVCC

Orange: so both will need to remove context

revised to 3128

**Decision:** The document was **revised to S3-183128**.

**S3-183128 Security procedure when returns to E-UTRAN or NR from UTRAN**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Huawei, Hisilicon*

(Replaces S3-182890)

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

**S3-182891 Security procedure when returns to E-UTRAN or NR from UTRAN**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Huawei, Hisilicon*

**Decision:** The document was **revised to S3-183129**.

**S3-183129 Security procedure when returns to E-UTRAN or NR from UTRAN**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Huawei, Hisilicon*

(Replaces S3-182891)

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

**S3-182991 Proposed change to the key derivation in solution #1.1 of TR 33.856**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Qualcomm Incorporated*

**Discussion:**

QC presents

E//: impact on AMF

QC: yes

E//: this has impact on 5G security, add editor's note on this

Orange: put this into the conclusion

QC: put note in conclusion it is possible to use different FC value

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

**S3-182892 Additional impacts on existing nodes and functionality for each solution**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

VF: "it needs to" needs to be fixed

Orange: ed note impact on 5G system needs to be evaluated

revised to 3131

**Decision:** The document was **revised to S3-183131**.

**S3-183131 Additional impacts on existing nodes and functionality for each solution**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Huawei, Hisilicon*

(Replaces S3-182892)

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

**S3-182992 Proposed resolution of the editor’s note in the conclusion clause of TR 33.856**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Qualcomm Incorporated*

**Discussion:**

QC presents

Orange: put editors note of 991 here, impact of different FC value is to be reviewed

E//: the new FC value has impact on 5G system

BT: prohibition to change 5G system on operators not deploying this, ok with editor's note

VF: Englishification

Orange: keep editor's note at the end

revised to 3130

**Decision:** The document was **revised to S3-183130**.

**S3-183130 Proposed resolution of the editor’s note in the conclusion clause of TR 33.856**

 *Type: pCR For: Approval
 33.856 v1.0.0
 Source: Qualcomm Incorporated*

(Replaces S3-182992)

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

**S3-183067 Draft TR 33.856**

 *Type: draft TR For: Approval
 33.856 v1.1.0
 Source: Huawei*

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

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

**S3-182803 New KI proposal for TR 33.861 on CIoT security - infrequent small data transmissions for low complexity UEs**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

**Abstract:**

This contribution proposes a new KI for TR 33.861.

**Discussion:**

T-Mobile USA presents

Alibaba: 3rd security requirement, CIoT devices may have different levels of security

Orange: not ok for security level to be less. Otherwise show that 5G security is not impacted

VF: all of this was already in best study, so reference would be better. disagree with document

BT: if infrequent data transmission, then not a ddos; may increase latency compared to what

NEC: number of comments

noted

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

**S3-182931 Key issue proposal for FS\_CIoT\_sec\_5G**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: NEC Europe Ltd*

**Abstract:**

This pCR proposes a key issue for study item on on evolution of Cellular IoT security for the 5G System (TR 33.861).

**Discussion:**

NEC try to merge into 805

VF: first sentence should go away.

E//: what does the sentence imply about integrity protection,is it bad?

NEC: impact on performance

E//: already introduced for this use case in GSM

QC: not understand the relationship between the clauses

E//: capture the difference between frequent and infrequent data transmission; this address more use cases.

Noted

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

**S3-182805 New KI proposal for TR 33.861 on CIoT security - frequent small data transmissions for low complexity UEs**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

**Abstract:**

This contribution proposes a new KI for TR 33.861.

**Discussion:**

T-Mobile USA presents

VF: how to have frequent data transmission in power constrained devices; should be two different key issues, one on frequent transmission, one on battery constrained.

VF: work to update key issue details

BT: second potential requirement is not security related

VF: threats: not clear what is important in data latency

BT: there may be a solution increasing latency

Orange: last requirement is shall

QC: all key issues are shalls

Nokia: but not for all requirements

taken offline

**Decision:** The document was **revised to S3-183132**.

**S3-183132 New KI proposal for TR 33.861 on CIoT security - frequent small data transmissions for low complexity UEs**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

(Replaces S3-182805)

**Discussion:**

T-Mobile USA presents draft

Orange: remove from IoT devices in requirement

E//: remove requirement 2

approved

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

**S3-182806 New KI proposal for TR 33.861 on CIoT security - Security-related signaling and authentication credentials management overhead**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

**Abstract:**

This contribution proposes a new KI for TR 33.861.

**Discussion:**

T-Mobile USA presents

Orange: this part of the work is led by SA2

VF: same opinion

T-Mobile: how about first requirement

Orange: impact for all Ues

DCM: what is the limit in the first requirement

VF: there should not be a separate key issue

Alibaba: what about devices which are power constraint, there is a basic requirement on 10 years battery lifetime for those devices.

DCM: go to R10 M2M requirement to get inspiration

noted

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

**S3-182856 pCR to TR33.861: Authentication of a group of CIoT devices**

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

**Discussion:**

Huawei presents, 2 paragraphs of key issue are not part of contribution, should be ignored

Orange: group authentication to replace individual authentication?

Huawei: not replace

Orange: this is going beyond the requirement from SA1

VF: all should be deleted, the concept of group authentication is not in scope, as the whole group concept has large impact

CMCC: group authentication to maintain a group, so not replace the individual authentication even if group authentication is not after individual authentication

Alibaba: should be studied

E//: group communication is out of scope, no requirement for group communication from SA1

Orange: key issue only acceptable that each UE is individually authenticated

DCM: progress this with conf calls, split out into separate key hierarchy

Huawei: there is the SA1 requirement

E//: not for group authentication, but authentication of groups.

taken offline

Huawei: conference calls needed to progress

noted

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

**S3-182949 Discussion on User authentication support for IoT devices**

 *Type: discussion For: Discussion
 33.861 v..
 Source: LG Electronics*

**Discussion:**

LG presents

VF: biometrics was objected to in San Diego, why is there user authentication in IoT

LG: there is a service requirement, so send LS to SA1

Orange: no, b should be ruled out, c: biometrics should not be collected by service provider, a: pin code i salready there

Orange: ignore the requirement

noted

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

**S3-182950 LS on clarification of user authentication requirement for IoT devices**

 *Type: LS out For: Approval
 to SA1
 Source: LG Electronics*

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

**S3-183021 New key issue for integrity protection of small data**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

Orange: only support, how about use

E//: support mandatory, use optional

Orange: add additional requirement for signalling, do that in next meeting

VF: endpoints of integrity protection undefined

E//: add between UE and network

Huawei: overlapping contribution 924

taken together with 924

**Decision:** The document was **revised to S3-183133**.

**S3-183133 New key issue for integrity protection of small data**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

(Replaces S3-183021)

**Discussion:**

E// presents draft

Orange add integrity protection

approved

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

**S3-183022 New key issue for encryption of small data**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

VF: encryption and decryption

E//: confidentiallity requirement.

Approved

**Decision:** The document was **revised to S3-183134**.

**S3-183134 New key issue for encryption of small data**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

(Replaces S3-183022)

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

**S3-182924 Key issue on security for small data transmission**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

Orange: fine with first requirement

E//: merge into 3021 and 3022, but have different key issues on confidentiality and integrity

VF: problems with threats and key issue wording

integrity requirements merged into 3133

confidentiality requirements merged into 3134

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

**S3-182801 New KI proposal for TR 33.861 on CIoT security – data transmission for frequent small data for low complexity UEs**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

**Abstract:**

This contribution proposes a new KI for TR 33.861.

**Discussion:**

T-Mobile USA presents

VF: same problem with power constrained devices, but then adding many packets, this is protected already

Orange: dealt with integrity and confidentiality, missing may be replay protection, 5G CiOT system doesn't exist

only replay protection merged into 3133

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

**S3-182804 New KI proposal for TR 33.861 on CIoT security - transmission types for infrequent small data for low complexity UEs**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

**Abstract:**

This contribution proposes a new KI for TR 33.861.

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

**S3-182857 pCR to TR33.861: Secure Communication for a group CIoT devices**

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

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

**S3-183010 Discussion on dealing with maliciously behaving devices in 5G networks**

 *Type: discussion For: Discussion
 33.861 v..
 Source: KPN N.V.*

**Abstract:**

This paper discusses the need for dealing with maliciously behaving devices and proposes a structural approach to solutions for these devices

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

**S3-183011 New Key Issue: Dealing with Malicious Applications on the UE**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: KPN N.V.*

**Abstract:**

This contribution proposes a new key issue related to malicious behaviour of devices, in particular to malicious applications on the UE.

**Discussion:**

KPN presents

VF: signalling storm is not well defined term, signalling overload, title signalling overload due to malicious applications on UE

Huawei: is this about signalling storm to application? If not merge with Huawei contribution

E//: remove requirement, clarify for next meeting

VF: there is also a second kind of signalling overload which is recovery from network coverage loss.

Lenovo: other groups should take care of this

E//: problem is wording of requirement

QC: overload controlwas there already in 4G

revised 3135

**Decision:** The document was **revised to S3-183135**.

**S3-183135 New Key Issue: Dealing with Malicious Applications on the UE**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: KPN N.V.*

(Replaces S3-183011)

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

**S3-182846 Key issue on massive registration**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

ZTE presents

Orange: first requirement is SA2 not SA3; not clear what is illegal registration in second point

noted

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

**S3-182858 Key Issue on gNB Protection from CIoT DoS attack**

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

**Discussion:**

Huawei presents

QC: this is already assuming we are doing at gNB

VF: formatting: 5.x.2 is indented

E//: first sentence of requirement not needed; rephrase to DoS against RAN

DCM: keep the RRC messages part

revised to 3136

**Decision:** The document was **revised to S3-183136**.

**S3-183136 Key Issue on gNB Protection from CIoT DoS attack**

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

(Replaces S3-182858)

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

**S3-182923 Key issue on DoS attack on the network for CIoT**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

QC: what is the difference from KPN document

Huawei: this is more specific

KPN: more focussed on security

Huawei: this one has the requirement

VF: 5G system is already able to deal with large numbers of devices

DCM: this is DDoS specific

VF: no difference between IoT and eMBB

T-Mobile: difference in scale

DCM: have discussion paper to go into key issue detail to describe the specifics of IoT

CMCC: problem with scale

Juniper: set the bar higher to describe that the requirement is different from non IoT.

Orange: agree with VF, DoS attacks not defended against on protocol layer, also using specialized equipment

Huawei: this is study, so not be too detailed

Orange: too much time taken for these

DCM: make a list of 5G system security requirements and use that as baseline,

BT: most problems are with bad IoT device implementations, so leverage Tc cyber hardening work.

E//: not leverage on existing requirements, because architecture is different

Orange: only different procedures, not different architecture

VF: take 5G system as baseline, look at differences

QC: note this and come back next meeting

Orange: should be in scope of 3GPP, the way it is written it is not

DCM: some solutions require protocol support

Orange: merge with KPN contribution

E//: malicious applications

DCM: note for now, come back next time offline

kept open

noted

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

**S3-183019 New key issue for security key storage**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

Idemia: no need for talking about authentication here

Gemalto: no need for such a key issue

E//: remove authentication

Orange: remove all of the key issue

VF: KI should be about frequent change of keys

noted

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

**S3-182896 Key Issue on IoT Terminal Security Monitoring**

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

**Discussion:**

Huawei presents

VF: what is the difference to ordinary network operations

Orange: agree, how is an IoT terminal identified

VF: IoT special use case, IoT device operators want to know about how well they are doing

Huawei: not part of 3GPP

noted

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

**S3-182843 Key issu-Avoiding AS security when application security enabled**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Discussion:**

Nokia presents

BT: concern that customer is managing operators security

E//: we already have this in 5G. Reomve last two bullets

Orange: no, not remove them. Last requirement is shall. Remove second requirement.

BT: remove first requirement

Orange: remove requirement

all requirements removed

approved as 3170

**Decision:** The document was **revised to S3-183170**.

**S3-183170 Key issu-Avoiding AS security when application security enabled**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182843)

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

**S3-183018 New key issue for security key refreshing**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

Orange: issue on session keys, not long term keys, add text

E//: ok

Huawei: KI is solution specific, needs to be rephrased

VF: issue with key issue details, security measures are often customer requirements, two editor's notes

Idemia: session keys everywhere

revised to 3171

**Decision:** The document was **revised to S3-183171**.

**S3-183171 New key issue for security key refreshing**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

(Replaces S3-183018)

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

**S3-182948 New key issue on secure provisioning of CIoT devices**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: LG Electronics*

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

**S3-182807 New KI proposal for TR 33.861 on CIoT security - secure provisioning of authentication credentials in the CIoT UEs**

 *Type: pCR For: Approval
 33.861 v12.0.0
 Source: InterDigital, Inc., T-Mobile USA*

**Abstract:**

This contribution proposes a new KI for TR 33.861.

**Discussion:**

T-Mobile USA presents

Orange: study item discussion in SA2: KIs linked to provisioning were agreed not to include. SA3 should do the same

T-Mobile: SA2 should do it then?

Orange: SA2 did not define a way of updating keys

Huawei: if SA3 doesn't do provisioning, where are the credentials coming from

VF: out of scope

noted

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

**S3-183020 New key issue for security key and authentication tag size**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

VF: which keys and tags are you talking about? Disagree with document

Orange: same feeling

VF: understand only in respect of privacy

Alibaba: maybe key length would be changed

E//: want to prevent shortening key length for efficiency purposes

VF: then it is ok

DCM: remove exponentially

Nokia: remove authentication tag size refers to solution

Idemia: remove authentication tag from title and text

**Decision:** The document was **revised to S3-183176**.

**S3-183176 New key issue for security key and authentication tag size**

 *Type: pCR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

(Replaces S3-183020)

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

**S3-182847 Key issue on overload control signalling protection**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

ZTE presents

QC: agreed a key issue on this already

Nokia: was noted

KPN: it was revised, this one is general overload control, problem is what is specifc to IoT

BT: mixing up deliberate attack and benign overload

noted

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

**S3-183012 New Solution: Procedure for detection of and response to signalling attacks on the Core Network**

 *Type: pCR For: Approval
 33.861 v0.0.0
 Source: KPN N.V.*

**Abstract:**

A proposed solution for handling malicious behaviour of UEs by detection of and response to signalling attacks on the Core Network

**Discussion:**

KPN presents, note this at the moment

VF: it is something to bring to SA2

noted

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

**S3-182895 Solution on Small Data Transfer for NAS Solution**

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

**Discussion:**

Huawei presents

VF: where is the other end of security, from NAS, how is data secured

Huawei: NDS/IP

VF: in roaming case, if customer doesn't want this in clear in the visited network

VF: how the data is secured from NAS to enterprise service is FFS

Huawei: not needed.

E//: this is the DoNAS solution

DCM: should or shall

Huawei: shall

E//: editor's note how to handle AMF relocation is FFS

revised to 3173 -> approved

**Decision:** The document was **revised to S3-183173**.

**S3-183173 Solution on Small Data Transfer for NAS Solution**

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

(Replaces S3-182895)

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

**S3-183068 Draft TR 33.861**

 *Type: draft TR For: Approval
 33.861 v0.1.0
 Source: Ericsson*

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

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

**S3-182815 LS reply to BBF Response to 3GPP SA2 liaison S2-183036 on ‘general status of work**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: S2-189038*

**Discussion:**

Huawei presents

Orange: SA2 is saying that SA3 is providing feedback which is funny

Orange: in this release, UEs will connect using 5G procedures with a UICC

E//: SA2 is considering FN-RG

Nokia: has to be resolved somehow

Orange: this is about authentication procedure,

BT: accept what is written in the LS about LI.

Idemia: all authentication is based on UICC

QC: only if 5G radio capability exists

Orange: storage not specified, but 5G authentication method is used.

QC: correct for R15, need to consider for R16.

BT: this is wireline, so do we want UICC on DECT phones

Orange: do we need to define something new.

BT: what about tethered services, do we want to force a new mechanism?

E//: not possible with legacy equipment.

Orange: do we need to standardize anything on the legacy devices?

Nokia: reply: we will study the mechanism of BBF and then decide

kept open

noted

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

**S3-182916 scope of TR33807**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei present

Orange: remove ie. Part

Orange remove non-3GPP part

E//: privacy objectives are combined, prefer to copy the complete objectives from SID

revised in 3137

**Decision:** The document was **revised to S3-183137**.

**S3-183137 scope of TR33807**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

(Replaces S3-182916)

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

**S3-182943 Discussion on approach to security solution for 5WWC**

 *Type: discussion For: Endorsement
 Source: NEC Europe Ltd*

**Abstract:**

This discussion tdoc analyses the corresponding SA2 to clarify security implications for the SA3 work in TR 33.807.

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

**S3-182944 pCR for KI on logical function support in 5WWC entities**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: NEC Europe Ltd*

**Abstract:**

This pCR proposes a new Key Issue on the logical function support in 5WWC entities from security perspective.

**Discussion:**

NEC presents

E//: good input, but not helpful for now

NEC: if N1, then it is normal UE,

Huawei: add editor's note: SA2 doesn't not define the interface

NEC: ok

BT: when work was done on HeNB, then there were constraints like spectrum only in one location, here this can be done easier

noted

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

**S3-182945 pCR for KI on relay function support in 5WWC**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: NEC Europe Ltd*

**Abstract:**

This pCR proposes a new Key Issue on the relay function support in 5WWC from security perspective.

**Discussion:**

NEC presents

NEC: need to ask SA2 to clarify relay aspects

Huawei: no need to send LS.

KPN: agree with NEC, because there are UE relays and radio relays

E//: is there no mention of what is in scope in the SA2 scope?

Orange: confused about support of relay function, therefore send LS to clarify.

E//: it is NECs interpretation that 5G-RG behaves as relay.

note this tdoc, take discussion about LS offline

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

**S3-182946 pCR for KI on FMC function support in 5WWC**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: NEC Europe Ltd*

**Abstract:**

This pCR proposes a new Key Issue on the FMC function support in 5WWC from security perspective.

**Discussion:**

NEC presents

Huawei: not clear, send LS

Orange: check specification first, before sending LS

noted

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

**S3-182907 new requirement of 5G RG**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

E//: is this about 5G RG authentication, but needs to clarified in the title

Orange: 5G-RG is like a 3GPP UE, so what is the difference

Nokia: more like a HeNB

DT: it is shall in requirement

E//: 5G-RG and network shall support authentication

Idemia: what is the 5G-RG, is it a device or a subscription

Nokia: NEC provides more detail

approved in 3138

**Decision:** The document was **revised to S3-183138**.

**S3-183138 new requirement of 5G RG**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

(Replaces S3-182907)

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

**S3-182970 New key issue: FN-RG authentication and authorization**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Ericsson*

**Discussion:**

E// presents

Orange: who authentciates the RG? Not comfortable with requirements

Huawei: overlapping contribution to be merged: 908

DCM: threat on authorization is badly formulated

E//: make it an editor's note

NEC: also fixed operator needs to ensure security, unclear who is responsible

Orange: for authentication procedure we are dependent on SA2, remove security requirements

together with 908

revised to 3139

**Decision:** The document was **revised to S3-183139**.

**S3-183139 New key issue: FN-RG authentication and authorization**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Ericsson*

(Replaces S3-182970)

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

**S3-182908 new requirement of FN-RG security**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: what is FMIF, solution specifc, merge with 970

DCM: threat not matching key issue

DCM: FN-RG not under operator control, therefore signalling overload possible - different key issue, come back next time.

Noted

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

**S3-182909 new requirement of devices behind a 5G-RG or a FN-RG**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: why is a new authentication method required? Disagree with document

Nokia: reduce to shall be authenticated

Orange: requirement not required

Nokia: may change things in the core

NEC: there is distinction between 5G and non 5G UE.

Orange: all 5G, but not all support 5G radio capabilities

NEC: these descriptions need to be captured

Lenovo: how is this related to the key issue, not support for this tdoc

noted

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

**S3-182808 New KI proposal for TR 33.807 - efficient security overhead for Wireless and Wireline Convergence in 5G**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: InterDigital, Inc.*

**Abstract:**

This contribution proposes a new KI for TR 33.807.

**Discussion:**

T-Mobile USA presents

DT: very vague requirements, note document

Orange: same

noted

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

**S3-182910 new requirement in key hierarchy**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: should->shall

DCM: completely unclear how it is written, key issue is not clear, threat is vague

noted

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

**S3-182911 new requirement in NAS security**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

DT: requirements ununderstandable

Orange: same

noted

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

**S3-182912 new requirement in multi NAS connection**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: where does multi-NAS security come from in this document?

E//: hybrid access is different than what is described here

noted

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

**S3-182913 new requirement in UP security**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: what should be aligned in security mechanism

DCM: KI details need rewording, threats need rewording, requirements need to be deleted

noted

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

**S3-182914 new requirement in IPTV supported**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: is there a solution for IPTV in TR already

NEC: MBMS is used for IPTV

BT: there may be different content protection in place for IPTV content

E//: is this for user plane with a particular application on top

Orange: remove the requirement

DCM: not clear what is the key issue, remove the needs to be studied, englishify

QC: is it IPTV or multicast

Huawei: IPTV in SA2

revised to 3140

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

**S3-183140 new requirement in IPTV supported**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

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

**S3-182971 New key issue: Transport security for the interfaces between W-5GAN and 5GC**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Ericsson*

**Discussion:**

E// presents

QC: shorten Security threat

Orange: replace encryption by confidentiality protection

Orange: remove indentation

revised to 3141

**Decision:** The document was **revised to S3-183141**.

**S3-183141 New key issue: Transport security for the interfaces between W-5GAN and 5GC**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Ericsson*

(Replaces S3-182971)

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

**S3-182972 New key issue: Security for the interface between 5G-RG and W-5GAN**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Ericsson*

**Discussion:**

E// presents

QC: same comment as in 971, shorten threat

approved as 3144

**Decision:** The document was **revised to S3-183144**.

**S3-183144 New key issue: Security for the interface between 5G-RG and W-5GAN**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Ericsson*

(Replaces S3-182972)

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

**S3-182939 Definitions and abbreviations for trusted access**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility, Lenovo*

**Abstract:**

This paper introduces definitions and abbreviations used in TR 23.716 for trusted non-3GPP access.

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

**S3-182938 Key Issue on Registration and NAS transport for trusted non-3GPP access**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility, Lenovo*

**Abstract:**

Proposes a new key issue for trusted non-3GPP access.

**Decision:** The document was **revised to S3-183145**.

**S3-183145 Key Issue on Registration and NAS transport for trusted non-3GPP access**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility, Lenovo*

(Replaces S3-182938)

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

**S3-182915 new requirement in truted access**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Huawei, Hisilicon*

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

**S3-182940 Solution for trusted access**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility UK Ltd.*

**Abstract:**

This paper introduces a solution for trusted access according to the conclusions of TR 23.716.

**Discussion:**

Lenovo presents

E//: what is change to SA2 solution, editor's note the difference to solution 7.1 of TR whatever of SA2 needs to be made clear

**Decision:** The document was **revised to S3-183146**.

**S3-183146 Solution for trusted access**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility UK Ltd.*

(Replaces S3-182940)

**Discussion:**

Lenovo presents draft

Orange: ed note misleading

approved

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

**S3-183069 Draft TR 33.807**

 *Type: draft TR For: Approval
 33.807 v0.1.0
 Source: Huawei*

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

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

**S3-182816 Reply LS on clarification on Restricted Operator Services**

 *Type: LS in For: (not specified)
 Original outgoing LS: -, to -, cc -
 Source: S2-181407*

**Discussion:**

QC presents

BT: integrity protection can't be provided with preconfigured Null algorithm, that is completely untrue

QC: it just says that null is used

Sprint: response not needed from this meeting, because SA2 is not working on this this quarter

postponed

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

**S3-182844 PARLOS Key issue: Providing temperory security for unauthenticated UEs**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Nokia, Nokia Shanghai Bell*

**Abstract:**

Add new key issue

**Discussion:**

Nokia presents

BT: include integrity in the threats sections

E//: only keep third requirement

Nokia: ok, that is the main requirement

Lenovo: AS and NAS security should be protected, add requirement

QC: how can this be achieved

Lenovo: there is a contribution in this meeting

VF: insecure interfaces causes a lot problems, so support Lenovo

E//: how could we solve this, and can we have a requirement if there is no solution

DCM: yes, if requirement can't be fulfilled, we may decide to accept the risk or not do it.

Orange: where do you want to establish security to

Nokia: there is a RLOS portal

E//: could be IMS as well

E//: many spelling errors

E//: AS and NAS security may not be possible instead of is not possible

revised to 3149

**Decision:** The document was **revised to S3-183149**.

**S3-183149 PARLOS Key issue: Providing temperory security for unauthenticated UEs**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Nokia, Nokia Shanghai Bell*

(Replaces S3-182844)

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

**S3-182864 EPC solution for RLOS access**

 *Type: pCR For: (not specified)
 33.815 v0.0.0
 Source: Intel Corporation (UK) Ltd*

**Discussion:**

Intel presents

Orange: modifying provisioning solution of GSMA, not the right place

noted

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

**S3-182871 Support for Unauthenticated UEs access to RLOS using EPC**

 *Type: pCR For: (not specified)
 33.815 v0.0.0
 Source: Intel Corporation (UK) Ltd*

**Discussion:**

Intel presents

E//: DoS threat to authorization requirement

Orange: agree, also delete threat

BT: need to protect the network

Orange: last sentence in key issue details is a requirement and a solution

revised in 3150

approved

**Decision:** The document was **revised to S3-183150**.

**S3-183150 Support for Unauthenticated UEs access to RLOS using EPC**

 *Type: pCR For: -
 33.815 v0.0.0
 Source: Intel Corporation (UK) Ltd*

(Replaces S3-182871)

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

**S3-182930 Key Issue on PARLOS Security**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Motorola Mobility, Lenovo*

**Abstract:**

Proposes a new key issue on PARLOS security.

**Discussion:**

Lenovo presents

NEC: requirement not clear, confidentiality and Integrity

E//: add whenever possible

DCM: exceptions are natural, don't add whenever possible

merged into 3149, only requirements

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

**S3-182932 PARLOS security solution**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Motorola Mobility, Lenovo*

**Abstract:**

Proposes a solution for AS and NAS security for RLOS.

**Discussion:**

Lenovo presents

E//: needs to clarify which key issue this solution addresses -> add editor's note, only protects against passive attacks

Orange: if public keys are signed by authorities trusted by UE then this is possible, -> editor's note

Gemalto: what is the difference between this solution and the Intel one.

Orange: works with trusted CA

E//: remove evaluation

Nokia: shift the evaluation sentences into precondition

offline

revised to 3151

**Decision:** The document was **revised to S3-183151**.

**S3-183151 PARLOS security solution**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Motorola Mobility, Lenovo*

(Replaces S3-182932)

**Discussion:**

Lenovo presents draft

E//: put x as key issue number

approved

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

**S3-182936 Key Issue on Access to 5GC from UEs that do not support NAS**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility, Lenovo*

**Abstract:**

Proposes a new key issue for UEs that do not support NAS for trusted non-3GPP access.

**Discussion:**

Lenovo presents

Huawei: title is too large, seems to cover wireline access

DCM: WLAN UEs in title

approved as 3147

**Decision:** The document was **revised to S3-183147**.

**S3-183147 Key Issue on Access to 5GC from UEs that do not support NAS**

 *Type: pCR For: Approval
 33.807 v0.0.0
 Source: Motorola Mobility, Lenovo*

(Replaces S3-182936)

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

**S3-182973 New key issue: Authentication between UE and EPC**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Ericsson*

**Discussion:**

E// presents

VF: key issue detail is irrelevant to the threat and requirements, so note document

Orange: doesn't under key issue details

noted

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

**S3-183054 Proposed TR Background Clause**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Sprint*

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

**S3-183055 Proposed TR Introduction Clause**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Sprint*

**Discussion:**

Sprint presents

Orange: what exactly is in the scope of this study

Sprint: regulatory requirement in the US, all kinds of access, cf. SA1 TS

VF: that is a study, so only possible services

Sprint: in the US, there is a requirement to at least provide outgoing calls

Orange: is TS22.011 defining Parlos?

VF: 22.011 is for network selection, there is one paragraph defining RLOS requirements

approved

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

**S3-183056 Proposed Requirements, assumptions, and constraints Clause**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Sprint*

**Discussion:**

Sprint presents

Orange: should be in SA1, note

Sprint: ok, might come back if not in SA1 scope

noted

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

**S3-183057 Proposed Scope Clause**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Sprint*

**Discussion:**

Sprint presents

E//: copy the objective as scope

Orange: agree

keep open

offline

**Decision:** The document was **revised to S3-183175**.

**S3-183175 Proposed Scope Clause**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Sprint*

(Replaces S3-183057)

**Decision:** The document was **revised to S3-183177**.

**S3-183148 Draft TR 33.815**

 *Type: draft TR For: Approval
 33.815 v0.1.0
 Source: Sprint*

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

**S3-183177 Proposed Scope Clause**

 *Type: pCR For: Approval
 33.815 v0.0.0
 Source: Sprint*

(Replaces S3-183175)

**Discussion:**

Sprint presents

DCM: first phrase is not a sentence

fix for next meeting

approved

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

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

**S3-182848 Key issue on protocol used for bootstrapping procedures**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: ZTE Corporation*

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

**S3-182849 Key issue on transaction ID generation**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: ZTE Corporation*

**Discussion:**

ZTE presents

Orange: different and solution specific, object

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

**S3-182899 Key Issue on mutual authentication between UE and BSF**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

Orange: solution specific

CMCC: replace BSF by anchor function

Orange: generalize it offline

Huawei: modify BSF to anchor function

DCM: rewrite threats to make better understandable

Orange: can only go in if anchor function contribution is accepted

revised to 3155

**Decision:** The document was **revised to S3-183155**.

**S3-183155 Key Issue on mutual authentication between UE and BSF**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: Huawei, Hisilicon*

(Replaces S3-182899)

**Discussion:**

Huawei presents draft

Orange: shall

approved

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

**S3-182925 Key issue on keys used in GBA**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: Huawei, HiSilicon*

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

**S3-182926 Key issue for fitting GBA into 5G core network functions**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

Orange: exactly same as 3091

Nokia: agree

DT: same handling as 3091

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

**S3-182947 New key issue on privacy of subscription and application users**

 *Type: pCR For: Approval
 33.835 v0.0.0
 Source: LG Electronics*

**Discussion:**

LG: already merged in 3006 after previous meeting, noted

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

**S3-182982 Key Issue for fitting BEST into 5G system**

 *Type: pCR For: Approval
 33.835 v12.0.0
 Source: Alibaba (China) Group., Ltd.*

**Discussion:**

revised due to offline comments

**Decision:** The document was **revised to S3-183091**.

**S3-183091 Key Issue for fitting BEST into 5G system**

 *Type: pCR For: Approval
 33.835 v12.0.0
 Source: Alibaba (China) Group., Ltd.*

(Replaces S3-182982)

**Discussion:**

Alibaba presents

DCM: what kind of security is meant

E//: this is really a solution

Orange: similar opinion

Nokia: enhancement of BEST for 5G sould not be part of this SID, should be separate SID

Alibaba: ?

Orange: best is a solution

CMCC: change the title, keep the requirements

CMCC: title: communincation protection between ...

Orange: if concentration on communication, then come back next time

Alibaba: important how to use BEST in the architecture. maybe discuss offline

Orange: offline to next meeting, because not enogh time to analyse a revision

Nokia: note, work till next meeting

noted

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

**S3-182983 Key Issue on secure communication between UE and enterprise application server**

 *Type: pCR For: Approval
 33.835 v12.0.0
 Source: Alibaba (China) Group., Ltd.*

**Discussion:**

revised due to offline comments

**Decision:** The document was **revised to S3-183092**.

**S3-183092 Key Issue on secure communication between UE and enterprise application server**

 *Type: pCR For: Approval
 33.835 v12.0.0
 Source: Alibaba (China) Group., Ltd.*

(Replaces S3-182983)

**Discussion:**

Alibaba presents

Orange: diagree with talking about cost and OPEX, solution specific requirement, keep the threats but not requirements

VF: second last paragraph of key issue details is not true, remove and the following one.

Remove requirements and last two paragraphs KI

taken offline

VF: should Best and GBA be split into separate studies.

Orange: In our key issue, we should be generic

VF: should we have a stdy on BEST for 5G

**Decision:** The document was **revised to S3-183158**.

**S3-183158 Key Issue on secure communication between UE and enterprise application server**

 *Type: pCR For: Approval
 33.835 v12.0.0
 Source: Alibaba (China) Group., Ltd.*

(Replaces S3-183092)

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

**S3-183000 Key Issue on secure communication between UE and 3rd party application server**

 *Type: pCR For: (not specified)
 33.835 v0.5.0
 Source: China Mobile, Alibaba (China) Group., Ltd., BT*

**Discussion:**

CMCC presents

Orange: this is solution specific, not a KI

Orange: what is generic about this threat and the requirement

Alibaba: then remove the example

Orange: threat here is similar to the one 3092

Alibaba: similar to anchor contribution

Orange: different with an additional function, not needed

Alibaba contribution is fine

merged in 3158

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

**S3-183004 Key Issue on secure communication between UE and 3rd party application server**

 *Type: pCR For: (not specified)
 33.835 v12.0.0
 Source: China Mobile, Alibaba (China) Group., Ltd., BT*

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

**S3-183005 Discussion and pCR for secure transferring between network and 3rd party in AKMA**

 *Type: pCR For: (not specified)
 33.835 v12.0.0
 Source: China Mobile, DT, KPN, LG electronics, Alibaba (China) Group., Ltd.*

**Discussion:**

CMCC presents

Orange: when talking about applicaiton server, is this the application function of SBA

VF: which bit of 3GPP network

DCM: AKMA function instead of 3GPP network

E//: there is a confusion, there is a E// contribution 3038 that can address this

BT: mixing it up with SBA applications

discussed with 3038

merged into 3160

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

**S3-183006 Discussion and pCR for identity key issue of AKMA**

 *Type: pCR For: (not specified)
 33.835 v12.0.0
 Source: China Mobile, DT, KPN, Alibaba (China) Group., Ltd.*

**Discussion:**

CMCC presents

E//: overlapping with 3012

CMCC: discuss all 5 overlapping documents at once.

Together with 2947, 3028, 849

E//: CMCC put everything in one key issue, E// more piecemeal

Orange: support SUPI as identifier, not share with other entitities

approved

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

**S3-183007 Discussion and pCR for decoupling secure procedure with specific protocol in AKMA**

 *Type: pCR For: (not specified)
 33.835 v12.0.0
 Source: China Mobile, KPN, LG electronics, Alibaba (China) Group., Ltd.*

**Discussion:**

CMCC presents

Orange: transport or security protocol

CMCC: transport

Orange: transport normally not specified by SA3

QC: AKMA should work over IP and non-IP

DCM: architectural requirements, remove requirements themselves and change title

approved as 3162

**Decision:** The document was **revised to S3-183162**.

**S3-183162 Discussion and pCR for decoupling secure procedure with specific protocol in AKMA**

 *Type: pCR For: -
 33.835 v12.0.0
 Source: China Mobile, KPN, LG electronics, Alibaba (China) Group., Ltd.*

(Replaces S3-183007)

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

**S3-183008 Candidate solution of introducing third party key to AKMA**

 *Type: pCR For: (not specified)
 33.835 v12.0.0
 Source: China Mobile*

**Discussion:**

CMCC presents

Orange: remove evaluation

Nokia: change title to include GBA

CMCC: here GBA is just an example

Alibaba: need to consider GBA-U as well. Ed. Note on GBA,

QC: that is a separate solution.

Alibaba: specifically describe what is the thrid party application server

QC: it's there, middle box in figure

CMCC: add editor's note?

revised to 3163

**Decision:** The document was **revised to S3-183163**.

**S3-183163 Candidate solution of introducing third party key to AKMA**

 *Type: pCR For: -
 33.835 v12.0.0
 Source: China Mobile*

(Replaces S3-183008)

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

**S3-183016 New KI: Key separation for AKMA AFs**

 *Type: pCR For: (not specified)
 33.835 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

QC: not required as requirement

BT: anchor or application function

E//: application function

DCM: spell out

approved as 3161

**Decision:** The document was **revised to S3-183161**.

**S3-183161 New KI: Key separation for AKMA AFs**

 *Type: pCR For: -
 33.835 v0.1.0
 Source: Ericsson*

(Replaces S3-183016)

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

**S3-183028 AKMA - new KI protecting long-term subscription identifiers**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

**Abstract:**

This pCR proposes a requirement that the system shall support protecting the long-term subscription identifiers used in the AKMA architecture.

**Discussion:**

E//: presents

Orange: in 5G there is only SUPI

QC, Huawei: same comment

noted

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

**S3-183029 AKMA - new KI privacy frirendly temporary subscription identifiers**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

**Abstract:**

This pCR proposes a requirement that the system shall support privacy friendly temporary subscription identifiers used in the AKMA architecture.

**Discussion:**

E// presents

Orange: valid key issue, but not temporary subscription identifiers

Huawei: what is privacy friendly

DCM: who is the attacker? Underspecified

noted

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

**S3-183030 AKMA - new KI protecting privacy in control and data traffic**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

**Abstract:**

This pCR proposes a requirement that the system shall support protecting the privacy sensitive content (other than identifiers) in control and data traffic used in the AKMA architecture.

**Discussion:**

E// presents

Orange: from where to where is the encryption required

E//: when mapped to GBA, the Z interfaces

BT: interpret this as referring third party should be focus

Nokia: UE to AKMA or to application layer

E//: both

Orange: remove first sentence

QC: other has to be removed in second sentence

revised to 3159 approved

**Decision:** The document was **revised to S3-183159**.

**S3-183159 AKMA - new KI protecting privacy in control and data traffic**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

(Replaces S3-183030)

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

**S3-183031 AKMA - new KI authentication framework**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

**Abstract:**

This pCR proposes a requirement that the system shall prevent a potential security compromise of AKMA authentication from propagating to the 3GPP primary authentication and NAS/AS security.

**Discussion:**

E//: presents

Orange: put in example in the key issue

Nokia: security threats: first one doesn't sound right, reviseit; remove vice versa from second threat

revised to 3156

**Decision:** The document was **revised to S3-183156**.

**S3-183156 AKMA - new KI authentication framework**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

(Replaces S3-183031)

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

**S3-183032 Key issue on AKMA architecture**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

**Abstract:**

This contribution proposes a new key issue on the need for an authentication anchor in the AKMA architecture.

**Discussion:**

E// presents

Orange: inthe security requirement: the anchor function can be standalone or existing

Alibaba: only Gba is described here

VF: spelling

CMCC: some more general solution desired

Huawei: related to 926

DCM: threats and requirement feel artificial

E//: then remove threats

DCM: requirement is architectural, add description of what anchor function means

China Telecom: look at interfaces and study these, related to 925, maybe merge

Orange: important that we have an anchor function

Huawei: remove figure, make requirement more general, because it is not clear if we need BSF or different function

Orange: figure is not important: important to keep an anchor function

E//: this is updating the key issues, different from Huawei and Alibaba key issues, which are more focussed

Nokia: not only relate text above figure to GBA or BEST etc. make it more generic

E//: fine if Nokia proposes additional text, e.g. on BEST architecture, important is need for anchor function

QC: keep the contribution

KPN: change title to anchor function

Huawei: remove figure, because it makes it look like standalone

E//: text clarifies that

DCM: add ed note for non-standalone figure

revised to 3154

QC: spelling

**Decision:** The document was **revised to S3-183154**.

**S3-183154 Key issue on AKMA architecture**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

(Replaces S3-183032)

**Discussion:**

E// presents draft

CMCC: potential architecture requirement

approved

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

**S3-183038 New KI: Protection of AKMA architecture interfaces**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

**Discussion:**

E// presents

VF: better than last one, add authentication to requirements

Orange: do we need requirements for non 3GPP controlled entities

QC: normally we do it

CMCC

revised to 3160

**Decision:** The document was **revised to S3-183160**.

**S3-183160 New KI: Protection of AKMA architecture interfaces**

 *Type: pCR For: Approval
 33.835 v0.1.0
 Source: Ericsson*

(Replaces S3-183038)

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

**S3-183157 Draft TR 33.835**

 *Type: draft TR For: Approval
 33.835 v0.1.0
 Source: China Mobile*

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

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

**S3-182831 Key Issue Contents “Termination points of N32 security”**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Deutsche Telekom AG*

**Abstract:**

This pCR proposes contents for the recently added key issue “Termination points of N32 security”.

**Discussion:**

Editorial corrections and approved in S3-183093

**Decision:** The document was **revised to S3-183093**.

**S3-183093 Key Issue Contents “Termination points of N32 security”**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Deutsche Telekom AG*

(Replaces S3-182831)

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

**S3-182832 Key Issue Contents “N32 error signalling”**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Deutsche Telekom AG*

**Abstract:**

This pCR proposes contents for the recently added key issue "N32 error signalling".

**Discussion:**

Ericsson: 2nd requirement needs something on error message -> revised in S3-183094

**Decision:** The document was **revised to S3-183094**.

**S3-183094 Key Issue Contents “N32 error signalling”**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Deutsche Telekom AG*

(Replaces S3-182832)

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

**S3-182833 New Key Issue "Modifications by authorized intermediaries on N32"**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Deutsche Telekom AG*

**Abstract:**

This pCR proposes a new key issue describing the need for modifications by authorized intermediaries on N32.

**Discussion:**

NCSC:Additonal requirement similar to "N32 security shall allow opertors to identify how IEs have been modified by authorised. Add fact that IE can't be modified. End of issue description needs modification. Nokia: 3rd requirement needs to go away. Revised to S3-183095

**Decision:** The document was **revised to S3-183095**.

**S3-183095 New Key Issue "Modifications by authorized intermediaries on N32"**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Deutsche Telekom AG*

(Replaces S3-182833)

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

**S3-182984 TLS and routing key issue**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Ericsson*

**Discussion:**

Nokia: Requirements into empty threat section- revised into S3-183096

**Decision:** The document was **revised to S3-183096**.

**S3-183096 TLS and routing key issue**

 *Type: pCR For: Approval
 33.855 v1.1.0
 Source: Ericsson*

(Replaces S3-182984)

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

**S3-183058 Draft TR 33.855**

 *Type: draft TR For: Approval
 33.855 v1.2.0
 Source: Deutsche Telekom*

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

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

**S3-182997 LTKUP: solution#5 evaluation against key issue #5**

 *Type: pCR For: Approval
 33.834 v0.7.0
 Source: Gemalto N.V.*

**Abstract:**

LTKUP: solution#5 evaluation against key issue #5

**Discussion:**

Gemalto presents

VF: wording he or she …

Orange: explain: the home operator can ask for new set of parameters

VF: from SIM suppliers

revised into 3152 and approved

**Decision:** The document was **revised to S3-183152**.

**S3-183152 LTKUP: solution#5 evaluation against key issue #5**

 *Type: pCR For: Approval
 33.834 v0.7.0
 Source: Gemalto N.V.*

(Replaces S3-182997)

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

**S3-183153 Draft TR 33.834**

 *Type: draft TR For: Approval
 33.834 v0.8.0
 Source: Vodafone*

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

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

**S3-182980 Minor corrections and clarifications to clauses 4.3, 5.1, 5.2, 6.2.2**

 *Type: pCR For: Approval
 33.841 v0.5.0
 Source: Ericsson*

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

**S3-183013 Key derivation function in TR 33.841**

 *Type: pCR For: (not specified)
 33.841 v0.5.0
 Source: China Mobile, Vodafone*

**Discussion:**

NCSC: Proposal contains more details than needed -> aim is to bring a simplified revised version at the next meeting.

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

**S3-182964 pCR to 33.841 - Addition of text for LTKUP impacts**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

**Discussion:**

Vdf presented. Recommendations do not belong in the modified clause. Proposal is to remove the recommendations and approved inlcuison of the rest. Orange: Why have LTKUP in this document when there is no normative work and it is not part of the 5G system? Agreement was to remove LTkUP stuff -> revised to S3-183165

**Decision:** The document was **revised to S3-183165**.

**S3-183165 pCR to 33.841 - Addition of text for LTKUP impacts**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

(Replaces S3-182964)

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

**S3-182961 pCR to TR 33.841- Clarification to section 7.1**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

**Abstract:**

Section 7.1 discusses attacks that become possible against a block cipher in counter mode, when the same counter block is used multiple times. The proposed revision clarifies the possible attacks and their implications.

**Discussion:**

Section 7.1 discusses attacks that become possible against a block cipher in counter mode, when the same counter block is used multiple times. The proposed revision clarifies the possible attacks and their implications.

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

**S3-182978 Clause 7.1.3: IV generation with randomizers**

 *Type: pCR For: Approval
 33.841 v0.5.0
 Source: Ericsson*

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

**S3-183014 MAC tag length implication on security - clarification to note**

 *Type: pCR For: Approval
 33.841 v0.5.0
 Source: NCSC*

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

**S3-182979 Clause 11: Desired performance aspects**

 *Type: pCR For: Approval
 33.841 v0.5.0
 Source: Ericsson*

**Discussion:**

proposed text for 11.3 was more about performance - it was agreed not to inlcude 11.3

**Decision:** The document was **revised to S3-183166**.

**S3-183166 Clause 11: Desired performance aspects**

 *Type: pCR For: Approval
 33.841 v0.5.0
 Source: Ericsson*

(Replaces S3-182979)

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

**S3-182965 pCR to 33.841 - Update to requirements section**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

**Discussion:**

There was some discussion on whether more than one authentication algorithm should be recommended. It was agreed to remove the last paragraph on the symmetric keys. There was some editorial corrections as well.

**Decision:** The document was **revised to S3-183167**.

**S3-183167 pCR to 33.841 - Update to requirements section**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

(Replaces S3-182965)

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

**S3-182966 pCR to 33.841 - section 15 - add initial conclusions**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

**Discussion:**

Vdf: Conclusions as written are all based on Quantum computing and indicate do nothing for 4 years. AT&T: May bring in non-quantum requirements in next meeting. NCSC: Change 'will' to 'may' of 5G symmetric algorithms - agreed. Orange: Think the symmetric conclusion could be worded more strongly. DCM: Proposed to delete the end of the first sentence. This was not agreeable

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

**S3-182962 LS on to RAN2/3 on the Impacts of increasing the MAC-I size**

 *Type: LS out For: Agreement
 to RAN2, RAN3, cc ETSI SAGE
 Source: Vodafone GmbH, AT&T*

**Discussion:**

Various editorial were made to the proposed LS - revised to S3-183168.

**Decision:** The document was **revised to S3-183168**.

**S3-183168 LS on to RAN2/3 on the Impacts of increasing the MAC-I size**

 *Type: LS out For: Agreement
 to RAN2, RAN3,CT1, cc ETSI SAGE
 Source: Vodafone GmbH, AT&T*

(Replaces S3-182962)

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

**S3-182963 pCR to 33.841 - Update to references Definitions and Abbreviations**

 *Type: pCR For: Agreement
 33.841 v0.5.0
 Source: Vodafone GmbH*

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

**S3-183169 Draft TR 33.841**

 *Type: draft TR For: Approval
 33.841 v0.6.0
 Source: Vodafone*

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

## 6 Any Other Business

Nokia: use groupings by rapporteurs based on input contributions in HTML file

Huawei: consider additional ad-hoc meetings

The chair thanks the organizers, the MCC replacement and the delegates for their hard work.

**S3-182850 skeleton of TS 33NEF**

 *Type: other For: Approval
 Source: ZTE Corporation*

**Discussion:**

ZTE presents

BT: typo in title: Explosure -> Exposure

approved as 3124

**Decision:** The document was **revised to S3-183124**.

**S3-183124 skeleton of TS 33NEF**

 *Type: draft TS For: Approval
 33.519 v0.1.0
 Source: ZTE Corporation*

(Replaces S3-182850)

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

**S3-182898 skeleton of KDF negotiation**

 *Type: other For: Information
 Source: Huawei, Hisilicon*

**Discussion:**

Huawei presents

QC: ed note should not mention 5WWC features

DCM: use clean TR template

Orange: candidate solutions

Orange: remove basis for normative work

approved as 3125

**Decision:** The document was **revised to S3-183125**.

**S3-183125 skeleton of KDF negotiation**

 *Type: draft TR For: Approval
 33.808 v0.1.0
 Source: Huawei, Hisilicon*

(Replaces S3-182898)

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

**S3-182928 skeleton of URLLC Study**

 *Type: other For: Information
 Source: Huawei, HiSilicon*

**Discussion:**

Huawei presents

same comments as in 898

approved as 3126

**Decision:** The document was **revised to S3-183126**.

**S3-183126 skeleton of URLLC Study**

 *Type: draft TR For: Approval
 33.825 v0.1.0
 Source: Huawei, HiSilicon*

(Replaces S3-182928)

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

**S3-182952 New WID on Addition of User Plane Integrity Protection in LTE and ENDC**

 *Type: WID new For: Agreement
 Source: Vodafone GmbH*

**Abstract:**

This draft WID proposes CR's to 33.401 to implement User Plane Integrity protection for LTE - 5G RAN combinations and LTE standalone.

**Discussion:**

VF presents

E//: start with study, deal with legacy equipment, legacy UEs

VF: primary target is EN-DC

E//: support this work, but start with study

BT: missing analysis whether the paper was fair, valid, impact, study on performance.

VF: there was a discussion document in the last meeting

Nokia: since IP in 5G is limited, then the attack scenario needs to be addressed

VF: conf call before the next meeting

DT: add notion of mandatory integrity protection, support study.

VF: feeling is this should be a SID, conf call on wording

Apple: evaluate the impact

Huawei: support this work.

Orange: also support

CMCC: support study

noted

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

**S3-183179 Procedure to deal with draft CRs from this meeting**

 *Type: other For: Information
 Source: WG Chair*

**Discussion:**

Chairman presents

Nokia: how to deal with revisions of text in current draft CRs?

Huawei: email approval of CRs?

DCM: if changes are required, it will be difficult

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

Report prepared by: Mirko Cano

## Annex A: List of contribution documents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document | Title | Source | Decision | Replaces | Replaced by |
| * S3-182800
 | * Agenda
 | * WG Chair
 | * approved
 |  |  |
| * S3-182801
 | * New KI proposal for TR 33.861 on CIoT security – data transmission for frequent small data for low complexity UEs
 | * InterDigital, Inc., T-Mobile USA
 | * merged
 |  | * S3-183133
 |
| * S3-182802
 | * The exposed I-RNTI issues in RRC resume procedure
 | * OPPO
 | * withdrawn
 |  |  |
| * S3-182803
 | * New KI proposal for TR 33.861 on CIoT security - infrequent small data transmissions for low complexity UEs
 | * InterDigital, Inc., T-Mobile USA
 | * noted
 |  |  |
| * S3-182804
 | * New KI proposal for TR 33.861 on CIoT security - transmission types for infrequent small data for low complexity UEs
 | * InterDigital, Inc., T-Mobile USA
 | * noted
 |  |  |
| * S3-182805
 | * New KI proposal for TR 33.861 on CIoT security - frequent small data transmissions for low complexity UEs
 | * InterDigital, Inc., T-Mobile USA
 | * revised
 |  | * S3-183132
 |
| * S3-182806
 | * New KI proposal for TR 33.861 on CIoT security - Security-related signaling and authentication credentials management overhead
 | * InterDigital, Inc., T-Mobile USA
 | * noted
 |  |  |
| * S3-182807
 | * New KI proposal for TR 33.861 on CIoT security - secure provisioning of authentication credentials in the CIoT UEs
 | * InterDigital, Inc., T-Mobile USA
 | * noted
 |  |  |
| * S3-182808
 | * New KI proposal for TR 33.807 - efficient security overhead for Wireless and Wireline Convergence in 5G
 | * InterDigital, Inc.
 | * noted
 |  |  |
| * S3-182809
 | * LS on Transmission mechanism of SUCI in NAS procedure
 | * C1-185663
 | * replied to
 |  |  |
| * S3-182810
 | * LS on Clarifications on SUPI definition and NAI format
 | * C4-186573
 | * noted
 |  |  |
| * S3-182811
 | * Reply LS on AUSF/UDM instance selection and SUCI parameters
 | * C4-186606
 | * noted
 |  |  |
| * S3-182812
 | * LS on Key Update
 | * R2-1813403
 | * replied to
 |  | * S3-183033
 |
| * S3-182813
 | * LS on Routing ID
 | * S2-188870
 | * noted
 |  |  |
| * S3-182814
 | * Reply to CT4 LS on Nausf\_SoRProtection service
 | * S2-189035
 | * noted
 |  |  |
| * S3-182815
 | * LS reply to BBF Response to 3GPP SA2 liaison S2-183036 on ‘general status of work
 | * S2-189038
 | * noted
 |  |  |
| * S3-182816
 | * Reply LS on clarification on Restricted Operator Services
 | * S2-181407
 | * postponed
 |  |  |
| * S3-182817
 | * LS on devices behind 5G-RG accessing the 5GC
 | * S3i180377
 | * noted
 |  |  |
| * S3-182818
 | * LS on SG17 work item X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
 | * ITU-T SG17
 | * postponed
 |  |  |
| * S3-182819
 | * Reply LS on Routing ID
 | * CP-182238
 | * replied to
 |  |  |
| * S3-182820
 | * Preference of protection policies on the N32 interface
 | * Deutsche Telekom AG
 | * revised
 |  | * S3-183083
 |
| * S3-182821
 | * Handling of encrypted IEs on the N32 interface
 | * Deutsche Telekom AG
 | * revised
 |  | * S3-183082
 |
| * S3-182822
 | * Update NDS/IP scope with application layer crypto profiles
 | * Juniper Networks, Ericsson
 | * revised
 |  | * S3-183122
 |
| * S3-182823
 | * Removal of Editor’s Note on security on the N32 interface
 | * Deutsche Telekom AG
 | * noted
 |  |  |
| * S3-182824
 | * Update references
 | * Juniper Networks, Ericsson
 | * revised
 |  | * S3-183121
 |
| * S3-182825
 | * Move TLS crypto profiles to TS 33.210
 | * Juniper Networks, Ericsson
 | * approved
 |  |  |
| * S3-182826
 | * Alignment of AS layer handling of EPS to 5GS handover with N2 handover
 | * CATT
 | * withdrawn
 |  |  |
| * S3-182827
 | * Correction to Nudm\_UEAuthentication\_ResultConfirmation service
 | * CATT
 | * withdrawn
 |  |  |
| * S3-182828
 | * Corrections to definition of 5G NAS security context
 | * CATT
 | * noted
 |  |  |
| * S3-182829
 | * Corrections to references for security related service in clause 14
 | * CATT
 | * approved
 |  |  |
| * S3-182830
 | * Modification on NAS SMC during multiple registrations in the same PLMN
 | * CATT
 | * noted
 |  |  |
| * S3-182831
 | * Key Issue Contents “Termination points of N32 security”
 | * Deutsche Telekom AG
 | * revised
 |  | * S3-183093
 |
| * S3-182832
 | * Key Issue Contents “N32 error signalling”
 | * Deutsche Telekom AG
 | * revised
 |  | * S3-183094
 |
| * S3-182833
 | * New Key Issue "Modifications by authorized intermediaries on N32"
 | * Deutsche Telekom AG
 | * revised
 |  | * S3-183095
 |
| * S3-182834
 | * Security Assurance Requirement and Test for AS NULL Integrity Disabling in the gNB
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182835
 | * Security Assurance Requirement and Test for failed Integrity Verification in the gNB
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182836
 | * Security Assurance Requirement and Test for synchronization failure handling in the UDM
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182837
 | * Security Assurance Requirement and Test for Kseaf Handling in the SEAF/AMF
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182838
 | * Security Assurance Requirement and Test for NAS NULL Integrity Disabling in the AMF
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182839
 | * Security Assurance Requirement and Test for RES\* verification failure handling in the AMF
 | * Nokia, Nokia Shanghai Bell
 | * noted
 |  |  |
| * S3-182840
 | * Security Assurance Requirement and Test for synchronization failure handling in the AMF
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183111
 |
| * S3-182841
 | * CR on Clarifictaions to Untrusted non-3GPP access clause
 | * Nokia, Nokia Shanghai Bell
 | * withdrawn
 |  |  |
| * S3-182842
 | * Discussion on LS S3-182809 timer on transmission of SUCI.
 | * Nokia, Nokia Shanghai Bell
 | * noted
 |  |  |
| * S3-182843
 | * Key issu-Avoiding AS security when application security enabled
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183170
 |
| * S3-182844
 | * PARLOS Key issue: Providing temperory security for unauthenticated UEs
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183149
 |
| * S3-182845
 | * Discussion on fast re-authentication
 | * ZTE Corporation, China Mobile, China Unicom
 | * noted
 |  |  |
| * S3-182846
 | * Key issue on massive registration
 | * ZTE Corporation
 | * noted
 |  |  |
| * S3-182847
 | * Key issue on overload control signalling protection
 | * ZTE Corporation
 | * noted
 |  |  |
| * S3-182848
 | * Key issue on protocol used for bootstrapping procedures
 | * ZTE Corporation
 | * noted
 |  | * -
 |
| * S3-182849
 | * Key issue on transaction ID generation
 | * ZTE Corporation
 | * noted
 |  |  |
| * S3-182850
 | * skeleton of TS 33NEF
 | * ZTE Corporation
 | * revised
 |  | * S3-183124
 |
| * S3-182851
 | * RRC Resume Request Authentication Token Calculation
 | * Huawei, HiSilicon
 | * noted
 |  |  |
| * S3-182852
 | * Update ResumeMAC-I calculation
 | * Huawei, HiSilicon
 | * noted
 |  |  |
| * S3-182853
 | * Update RNA Update Procedure Security
 | * Huawei, Hisilicon
 | * approved
 |  |  |
| * S3-182854
 | * Dual Connectivity Structure Update
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182855
 | * Intra-gNB-CU term synchronization
 | * Huawei, Hisilicon,
 | * approved
 |  |  |
| * S3-182856
 | * pCR to TR33.861: Authentication of a group of CIoT devices
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182857
 | * pCR to TR33.861: Secure Communication for a group CIoT devices
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182858
 | * Key Issue on gNB Protection from CIoT DoS attack
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183136
 |
| * S3-182859
 | * Update RRC reestablishment security procedure based on RAN2 agreement
 | * Huawei, Hisilicon
 | * postponed
 |  |  |
| * S3-182860
 | * DRAFT LS on ResumeMAC-I Calculation for RRC Resume Request
 | * Huawei, Hisilicon
 | * noted
 |  | * -
 |
| * S3-182861
 | * N2 HO: Handling source algorithms for RRC Reestablishment procedure
 | * Huawei, Hisilicon
 | * approved
 |  |  |
| * S3-182862
 | * NF discovery with SUCI
 | * NEC Corporation
 | * noted
 |  |  |
| * S3-182863
 | * Ciphering of user data between the UE and the gNB.
 | * NEC Corporation
 | * revised
 |  | * S3-183110
 |
| * S3-182864
 | * EPC solution for RLOS access
 | * Intel Corporation (UK) Ltd
 | * noted
 |  |  |
| * S3-182865
 | * Integrity protection of user data between the UE and the gNB
 | * NEC Corporation
 | * revised
 |  | * S3-183108
 |
| * S3-182866
 | * Replay protection of user data between the UE and the gNB
 | * NEC Corporation
 | * approved
 |  |  |
| * S3-182867
 | * Ciphering of RRC-signalling
 | * NEC Corporation
 | * revised
 |  | * S3-183109
 |
| * S3-182868
 | * Integrity protection of RRC-signalling
 | * NEC Corporation
 | * revised
 |  | * S3-183107
 |
| * S3-182869
 | * Replay protection of RRC-signalling
 | * NEC Corporation
 | * approved
 |  |  |
| * S3-182870
 | * Ciphering of user data based on the security policy sent by the SMF
 | * NEC Corporation
 | * approved
 |  |  |
| * S3-182871
 | * Support for Unauthenticated UEs access to RLOS using EPC
 | * Intel Corporation (UK) Ltd
 | * revised
 |  | * S3-183150
 |
| * S3-182872
 | * Integrity protection of user data based on the security policy sent by the SMF
 | * NEC Corporation
 | * approved
 |  |  |
| * S3-182873
 | * Confidentiality protection on the gNB DU-CU F1-U interface for user plane
 | * NEC Corporation
 | * noted
 |  |  |
| * S3-182874
 | * Integrity protection on the gNB DU-CU F1-U interface for user plane
 | * NEC Corporation
 | * noted
 |  |  |
| * S3-182875
 | * Replay protection on the gNB DU-CU F1-U interface for user plane
 | * NEC Corporation
 | * noted
 |  |  |
| * S3-182876
 | * Ciphering of NAS signalling message
 | * NEC Corporation, Deutsche Telekom AG
 | * revised
 |  | * S3-183112
 |
| * S3-182877
 | * Integrity protection of NAS signalling messages
 | * NEC Corporation, Deutsche Telekom AG
 | * revised
 |  | * S3-183113
 |
| * S3-182878
 | * Replay protection of NAS signalling messages
 | * NEC Corporation, Deutsche Telekom AG
 | * approved
 |  |  |
| * S3-182879
 | * Confidentiality protection of user data transported over N3 interface
 | * NEC Corporation, Samsung
 | * revised
 |  | * S3-183114
 |
| * S3-182880
 | * Integrity protection of user data transported over N3 interface
 | * NEC Corporation, Samsung
 | * revised
 |  | * S3-183115
 |
| * S3-182881
 | * Replay protection of user data transported over N3 interface
 | * NEC Corporation, Samsung
 | * revised
 |  | * S3-183116
 |
| * S3-182882
 | * Resolving the SUPI from the SUCI based on the protection scheme used to generate the SUCI
 | * NEC Corporation
 | * revised
 |  | * S3-183117
 |
| * S3-182883
 | * Storing authentication status of UE
 | * NEC Corporation
 | * revised
 |  | * S3-183118
 |
| * S3-182884
 | * Guidance on initial NAS message protection
 | * SP-180914
 | * replied to
 |  | * -
 |
| * S3-182885
 | * Alignment of AS layer handling of EPS to 5GS handover with N2 handover
 | * CATT
 | * merged
 |  | * S3-183070
 |
| * S3-182886
 | * Correction to Nudm\_UEAuthentication\_ResultConfirmation service
 | * CATT
 | * approved
 |  |  |
| * S3-182887
 | * Clarification on length of the ABBA parameter
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182888
 | * Discussion on the RI update requirement
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182889
 | * key isolation between AMFs when UDSF is deployed
 | * Huawei, Hisilicon
 | * withdrawn
 |  |  |
| * S3-182890
 | * Security procedure when returns to E-UTRAN or NR from UTRAN
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183128
 |
| * S3-182891
 | * Security procedure when returns to E-UTRAN or NR from UTRAN
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183129
 |
| * S3-182892
 | * Additional impacts on existing nodes and functionality for each solution
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183131
 |
| * S3-182893
 | * correction on the mobility from 5G to 4G
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183101
 |
| * S3-182894
 | * Involve Fresh Parameters to Input of InactiveMAC-I to Avoid Replay Attack
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182895
 | * Solution on Small Data Transfer for NAS Solution
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183173
 |
| * S3-182896
 | * Key Issue on IoT Terminal Security Monitoring
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182897
 | * RRC Reestablishment security handling when N2 Handover happens
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182898
 | * skeleton of KDF negotiation
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183125
 |
| * S3-182899
 | * Key Issue on mutual authentication between UE and BSF
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183155
 |
| * S3-182900
 | * Clarification on handover from EPS to 5GS
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183102
 |
| * S3-182901
 | * Editorial corrections on Authorization of NF service access
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183087
 |
| * S3-182902
 | * Handling for the service access failure
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182903
 | * Delete EN in SBA Requirements
 | * Huawei, Hisilicon
 | * approved
 |  |  |
| * S3-182904
 | * Topology hiding for SBA
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182905
 | * Add discover procedure as a pre-requisite for obtaining access token
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183088
 |
| * S3-182906
 | * Clarifications on AccessToken\_Get Response message
 | * Huawei, Hisilicon
 | * approved
 |  |  |
| * S3-182907
 | * new requirement of 5G RG
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183138
 |
| * S3-182908
 | * new requirement of FN-RG security
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182909
 | * new requirement of devices behind a 5G-RG or a FN-RG
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182910
 | * new requirement in key hierarchy
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182911
 | * new requirement in NAS security
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182912
 | * new requirement in multi NAS connection
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182913
 | * new requirement in UP security
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182914
 | * new requirement in IPTV supported
 | * Huawei, Hisilicon
 | * noted
 |  | * -
 |
| * S3-182915
 | * new requirement in truted access
 | * Huawei, Hisilicon
 | * withdrawn
 |  |  |
| * S3-182916
 | * scope of TR33807
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183137
 |
| * S3-182917
 | * UP security policy in NN-DC and MR-DC
 | * Huawei, Hisilicon
 | * revised
 |  | * S3-183106
 |
| * S3-182918
 | * Clafirication for ngKSI
 | * Huawei, Hisilicon
 | * merged
 |  | * S3-183076
 |
| * S3-182919
 | * Solution for RI update mechanism
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182920
 | * Editorial corrections on SoR
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182921
 | * Editorial corrections on the 5GS to EPS handover procedure
 | * Huawei, HiSilicon
 | * withdrawn
 |  |  |
| * S3-182922
 | * Clarification for Target to Source container
 | * Huawei, HiSilicon
 | * withdrawn
 |  |  |
| * S3-182923
 | * Key issue on DoS attack on the network for CIoT
 | * Huawei, HiSilicon
 | * noted
 |  |  |
| * S3-182924
 | * Key issue on security for small data transmission
 | * Huawei, HiSilicon
 | * merged
 |  | * S3-183134
 |
| * S3-182925
 | * Key issue on keys used in GBA
 | * Huawei, HiSilicon
 | * noted
 |  |  |
| * S3-182926
 | * Key issue for fitting GBA into 5G core network functions
 | * Huawei, HiSilicon
 | * noted
 |  |  |
| * S3-182927
 | * Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access
 | * Huawei, HiSilicon
 | * withdrawn
 |  |  |
| * S3-182928
 | * skeleton of URLLC Study
 | * Huawei, HiSilicon
 | * revised
 |  | * S3-183126
 |
| * S3-182929
 | * Editorial changes to the 5G AV definition
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182930
 | * Key Issue on PARLOS Security
 | * Motorola Mobility, Lenovo
 | * merged
 |  | * S3-183149
 |
| * S3-182931
 | * Key issue proposal for FS\_CIoT\_sec\_5G
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182932
 | * PARLOS security solution
 | * Motorola Mobility, Lenovo
 | * revised
 |  | * S3-183151
 |
| * S3-182933
 | * Editorial corrections on the 5GS to EPS handover procedure
 | * Huawei, HiSilicon
 | * revised
 |  | * S3-183103
 |
| * S3-182934
 | * Clarification for Target to Source container
 | * Huawei, HiSilicon
 | * revised
 |  | * S3-183104
 |
| * S3-182935
 | * Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access
 | * Huawei, HiSilicon
 | * revised
 |  | * S3-183119
 |
| * S3-182936
 | * Key Issue on Access to 5GC from UEs that do not support NAS
 | * Motorola Mobility, Lenovo
 | * revised
 |  | * S3-183147
 |
| * S3-182937
 | * Transmission mechanism of SUCI in NAS procedure
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182938
 | * Key Issue on Registration and NAS transport for trusted non-3GPP access
 | * Motorola Mobility, Lenovo
 | * revised
 |  | * S3-183145
 |
| * S3-182939
 | * Definitions and abbreviations for trusted access
 | * Motorola Mobility, Lenovo
 | * merged
 |  | * S3-183146
 |
| * S3-182940
 | * Solution for trusted access
 | * Motorola Mobility UK Ltd.
 | * revised
 |  | * S3-183146
 |
| * S3-182941
 | * SUCI freshness in registration procedure
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182942
 | * Achieving higher data rates for UP IP
 | * Motorola Mobility, Lenovo
 | * noted
 |  |  |
| * S3-182943
 | * Discussion on approach to security solution for 5WWC
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182944
 | * pCR for KI on logical function support in 5WWC entities
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182945
 | * pCR for KI on relay function support in 5WWC
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182946
 | * pCR for KI on FMC function support in 5WWC
 | * NEC Europe Ltd
 | * noted
 |  |  |
| * S3-182947
 | * New key issue on privacy of subscription and application users
 | * LG Electronics
 | * noted
 |  |  |
| * S3-182948
 | * New key issue on secure provisioning of CIoT devices
 | * LG Electronics
 | * noted
 |  |  |
| * S3-182949
 | * Discussion on User authentication support for IoT devices
 | * LG Electronics
 | * noted
 |  |  |
| * S3-182950
 | * LS on clarification of user authentication requirement for IoT devices
 | * LG Electronics
 | * noted
 |  |  |
| * S3-182951
 | * Correction to 5G AKA procedure - no need for "SUPI or SUCI"
 | * Orange
 | * approved
 |  |  |
| * S3-182952
 | * New WID on Addition of User Plane Integrity Protection in LTE and ENDC
 | * Vodafone GmbH
 | * noted
 |  |  |
| * S3-182953
 | * Clarification to key hierarchy description
 | * Nokia, Nokia Shanghai Bell
 | * noted
 |  |  |
| * S3-182954
 | * Corrections and additions in definitions and related clauses
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183072
 |
| * S3-182955
 | * Clarification to AUSF key derivation
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183097
 |
| * S3-182956
 | * Clarification to support of authentication methods
 | * Nokia, Nokia Shanghai Bell
 | * revised
 | * S3-182680
 | * S3-183077
 |
| * S3-182957
 | * Adding reference to 33.501 in 33.102
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182958
 | * Alignment regarding KEY reference to 33.220
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183098
 |
| * S3-182959
 | * Misleading text with reference regarding serving network name
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183099
 |
| * S3-182960
 | * Clarification on first bits of EMSK
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182961
 | * pCR to TR 33.841- Clarification to section 7.1
 | * Vodafone GmbH
 | * approved
 |  |  |
| * S3-182962
 | * LS on to RAN2/3 on the Impacts of increasing the MAC-I size
 | * Vodafone GmbH, AT&T
 | * revised
 |  | * S3-183168
 |
| * S3-182963
 | * pCR to 33.841 - Update to references Definitions and Abbreviations
 | * Vodafone GmbH
 | * withdrawn
 |  |  |
| * S3-182964
 | * pCR to 33.841 - Addition of text for LTKUP impacts
 | * Vodafone GmbH
 | * revised
 |  | * S3-183165
 |
| * S3-182965
 | * pCR to 33.841 - Update to requirements section
 | * Vodafone GmbH
 | * revised
 |  | * S3-183167
 |
| * S3-182966
 | * pCR to 33.841 - section 15 - add initial conclusions
 | * Vodafone GmbH
 | * noted
 |  |  |
| * S3-182967
 | * Removing mandatory text from note
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182968
 | * Reference correction
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182969
 | * The exposed I-RNTI issues in RRC resume procedure
 | * OPPO
 | * noted
 |  |  |
| * S3-182970
 | * New key issue: FN-RG authentication and authorization
 | * Ericsson
 | * revised
 |  | * S3-183139
 |
| * S3-182971
 | * New key issue: Transport security for the interfaces between W-5GAN and 5GC
 | * Ericsson
 | * revised
 |  | * S3-183141
 |
| * S3-182972
 | * New key issue: Security for the interface between 5G-RG and W-5GAN
 | * Ericsson
 | * revised
 |  | * S3-183144
 |
| * S3-182973
 | * New key issue: Authentication between UE and EPC
 | * Ericsson
 | * noted
 |  |  |
| * S3-182974
 | * Clarification to N32 Procedure on insertion of decrypted values
 | * Ericsson
 | * revised
 |  | * S3-183085
 |
| * S3-182975
 | * Length of IV salt and sequence counter
 | * Ericsson
 | * approved
 |  |  |
| * S3-182976
 | * Privacy - max. size of scheme-output for proprietary protection schemes
 | * Ericsson
 | * revised
 |  | * S3-183123
 |
| * S3-182977
 | * Privacy - LS on maximum output size of SUPI concealment schemes
 | * Ericsson
 | * revised
 |  | * S3-183142
 |
| * S3-182978
 | * Clause 7.1.3: IV generation with randomizers
 | * Ericsson
 | * approved
 |  |  |
| * S3-182979
 | * Clause 11: Desired performance aspects
 | * Ericsson
 | * revised
 |  | * S3-183166
 |
| * S3-182980
 | * Minor corrections and clarifications to clauses 4.3, 5.1, 5.2, 6.2.2
 | * Ericsson
 | * approved
 |  |  |
| * S3-182981
 | * PLMN ID protection in N32 message
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-182982
 | * Key Issue for fitting BEST into 5G system
 | * Alibaba (China) Group., Ltd.
 | * revised
 |  | * S3-183091
 |
| * S3-182983
 | * Key Issue on secure communication between UE and enterprise application server
 | * Alibaba (China) Group., Ltd.
 | * revised
 |  | * S3-183092
 |
| * S3-182984
 | * TLS and routing key issue
 | * Ericsson
 | * revised
 |  | * S3-183096
 |
| * S3-182985
 | * Token caching
 | * Ericsson
 | * revised
 |  | * S3-183089
 |
| * S3-182986
 | * NF instances in token claims
 | * Ericsson
 | * revised
 |  | * S3-183090
 |
| * S3-182987
 | * Remove EN in 13.2
 | * Nokia, Nokia Shanghai Bell
 | * approved
 |  |  |
| * S3-182988
 | * Clarifications to clause 13.2.x
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183078
 |
| * S3-182989
 | * Discussion on proposal for draft CR on option to derive partial context
 | * Qualcomm Incorporated
 | * noted
 |  |  |
| * S3-182990
 | * Acknowledging possibility of early calculation of EMSK
 | * Qualcomm Incorporated
 | * revised
 |  | * S3-183076
 |
| * S3-182991
 | * Proposed change to the key derivation in solution #1.1 of TR 33.856
 | * Qualcomm Incorporated
 | * approved
 |  |  |
| * S3-182992
 | * Proposed resolution of the editor’s note in the conclusion clause of TR 33.856
 | * Qualcomm Incorporated
 | * revised
 |  | * S3-183130
 |
| * S3-182993
 | * RRC Inactive security issue
 | * Qualcomm Incorporated
 | * noted
 |  |  |
| * S3-182994
 | * Key derivation in the RRC Inactive state
 | * Qualcomm Incorporated
 | * noted
 |  |  |
| * S3-182995
 | * MR-DC user plane integrity protection
 | * Qualcomm Incorporated
 | * merged
 |  | * S3-183106
 |
| * S3-182996
 | * Remove EN in clause 13.2.y.1
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183079
 |
| * S3-182997
 | * LTKUP: solution#5 evaluation against key issue #5
 | * Gemalto N.V.
 | * revised
 |  | * S3-183152
 |
| * S3-182998
 | * Correction in step 2 of 13.2.y.2
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183080
 |
| * S3-182999
 | * Corrections in 13.2.y.4 on N32-f context ID
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183081
 |
| * S3-183000
 | * Key Issue on secure communication between UE and 3rd party application server
 | * China Mobile, Alibaba (China) Group., Ltd., BT
 | * merged
 |  | * S3-183158
 |
| * S3-183001
 | * Clarifications and corrections in clause 13.2.a
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183127
 |
| * S3-183002
 | * pCR to S3-182700 regarding N32-f key hierarchy
 | * China Mobile
 | * revised
 |  | * S3-183084
 |
| * S3-183003
 | * N32 related definitions
 | * Nokia, Nokia Shanghai Bell
 | * noted
 |  | * -
 |
| * S3-183004
 | * Key Issue on secure communication between UE and 3rd party application server
 | * China Mobile, Alibaba (China) Group., Ltd., BT
 | * withdrawn
 |  |  |
| * S3-183005
 | * Discussion and pCR for secure transferring between network and 3rd party in AKMA
 | * China Mobile, DT, KPN, LG electronics, Alibaba (China) Group., Ltd.
 | * merged
 |  | * S3-183160
 |
| * S3-183006
 | * Discussion and pCR for identity key issue of AKMA
 | * China Mobile, DT, KPN, Alibaba (China) Group., Ltd.
 | * approved
 |  |  |
| * S3-183007
 | * Discussion and pCR for decoupling secure procedure with specific protocol in AKMA
 | * China Mobile, KPN, LG electronics, Alibaba (China) Group., Ltd.
 | * revised
 |  | * S3-183162
 |
| * S3-183008
 | * Candidate solution of introducing third party key to AKMA
 | * China Mobile
 | * revised
 |  | * S3-183163
 |
| * S3-183009
 | * Security aspects of SEPP - IPX communication
 | * Nokia, Nokia Shanghai Bell
 | * noted
 |  |  |
| * S3-183010
 | * Discussion on dealing with maliciously behaving devices in 5G networks
 | * KPN N.V.
 | * noted
 |  |  |
| * S3-183011
 | * New Key Issue: Dealing with Malicious Applications on the UE
 | * KPN N.V.
 | * revised
 |  | * S3-183135
 |
| * S3-183012
 | * New Solution: Procedure for detection of and response to signalling attacks on the Core Network
 | * KPN N.V.
 | * noted
 |  |  |
| * S3-183013
 | * Key derivation function in TR 33.841
 | * China Mobile, Vodafone
 | * noted
 |  |  |
| * S3-183014
 | * MAC tag length implication on security - clarification to note
 | * NCSC
 | * approved
 |  |  |
| * S3-183015
 | * Draft\_CR Corrections to Untrusted Non3GPP access clause
 | * Nokia, Nokia Shanghai Bell
 | * revised
 |  | * S3-183120
 |
| * S3-183016
 | * New KI: Key separation for AKMA AFs
 | * Ericsson
 | * revised
 |  | * S3-183161
 |
| * S3-183017
 | * Correction to the Security Service for Steering of Roaming
 | * Ericsson
 | * approved
 |  |  |
| * S3-183018
 | * New key issue for security key refreshing
 | * Ericsson
 | * revised
 |  | * S3-183171
 |
| * S3-183019
 | * New key issue for security key storage
 | * Ericsson
 | * noted
 |  |  |
| * S3-183020
 | * New key issue for security key and authentication tag size
 | * Ericsson
 | * revised
 |  | * S3-183176
 |
| * S3-183021
 | * New key issue for integrity protection of small data
 | * Ericsson
 | * revised
 |  | * S3-183133
 |
| * S3-183022
 | * New key issue for encryption of small data
 | * Ericsson
 | * revised
 |  | * S3-183134
 |
| * S3-183023
 | * AS sec – preventing "type confusion" attack between resume and re-establishment procedures
 | * Ericsson
 | * noted
 |  |  |
| * S3-183024
 | * AS sec – discussion on replay protection of inactiveMAC-I
 | * Ericsson
 | * noted
 |  |  |
| * S3-183025
 | * AS sec – integrity protection of traffic between UE and SN
 | * Ericsson
 | * noted
 |  |  |
| * S3-183026
 | * NAS key refresh
 | * Ericsson
 | * revised
 |  | * S3-183075
 |
| * S3-183027
 | * Mobility – Clarification of downlink NAS COUNT in N2 handover
 | * Ericsson
 | * approved
 |  |  |
| * S3-183028
 | * AKMA - new KI protecting long-term subscription identifiers
 | * Ericsson
 | * noted
 |  |  |
| * S3-183029
 | * AKMA - new KI privacy frirendly temporary subscription identifiers
 | * Ericsson
 | * noted
 |  |  |
| * S3-183030
 | * AKMA - new KI protecting privacy in control and data traffic
 | * Ericsson
 | * revised
 |  | * S3-183159
 |
| * S3-183031
 | * AKMA - new KI authentication framework
 | * Ericsson
 | * revised
 |  | * S3-183156
 |
| * S3-183032
 | * Key issue on AKMA architecture
 | * Ericsson
 | * revised
 |  | * S3-183154
 |
| * S3-183033
 | * Inteworking - reply LS on key update
 | * Ericsson
 | * revised
 |  | * S3-183071
 |
| * S3-183034
 | * Interworking - correcting keying material in HO request message (EPS to 5GS)
 | * Ericsson
 | * revised
 |  | * S3-183070
 |
| * S3-183035
 | * Update of EAP-AKA’ RFC 5448 in progress
 | * Ericsson
 | * noted
 |  |  |
| * S3-183036
 | * Work on improving perfect forward secrecy in 5G network access
 | * Ericsson
 | * noted
 |  |  |
| * S3-183037
 | * Using EAP-TLS with TLS 1.3
 | * Ericsson
 | * noted
 |  |  |
| * S3-183038
 | * New KI: Protection of AKMA architecture interfaces
 | * Ericsson
 | * revised
 |  | * S3-183160
 |
| * S3-183039
 | * Update of EAP-AKA’ reference to make it compatible with 5G
 | * Ericsson
 | * revised
 |  | * S3-183100
 |
| * S3-183040
 | * Modification of initial NAS message protection
 | * ZTE Corporation
 | * noted
 |  |  |
| * S3-183041
 | * Initial NAS – Discussion on Initial NAS protection
 | * Intel Corporation (UK) Ltd
 | * noted
 |  |  |
| * S3-183042
 | * Discussion of intial NAS message ciphering protection
 | * China Mobile
 | * noted
 |  |  |
| * S3-183043
 | * CR of update for all encryption for initial NAS message
 | * China Mobile
 | * noted
 |  |  |
| * S3-183044
 | * comments on Handling of encrypted IEs on the N32 interface
 | * NTT DOCOMO
 | * merged
 |  | * S3-183082
 |
| * S3-183045
 | * Comments on RRC Inactive security issue
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-183046
 | * Discussion on Protection of initial NAS message
 | * Huawei, Hisilicon
 | * noted
 |  |  |
| * S3-183047
 | * Analysing the impact of the plenary decision on the proposal for initial NAS security
 | * Qualcomm Incorporated
 | * noted
 |  |  |
| * S3-183048
 | * Correcting the description of the initial NAS protection method
 | * Qualcomm Incorporated
 | * noted
 |  |  |
| * S3-183049
 | * Nokia comments to S3-182888
 | * Nokia, Nokia Shanghai Bell
 | * noted
 |  |  |
| * S3-183050
 | * Discussion on LS on Routing ID Update
 | * Nokia, Nokia Shangahi Bell
 | * noted
 |  |  |
| * S3-183051
 | * A way forward for the initial NAS protection mechanism
 | * Ericsson
 | * noted
 |  |  |
| * S3-183052
 | * Backward compaitibility mechanism for the partial ciphering feature
 | * Ericsson
 | * revised
 |  | * S3-183053
 |
| * S3-183053
 | * Backward compaitibility mechanism for the partial ciphering feature
 | * Ericsson
 | * noted
 | * S3-183052
 | * -
 |
| * S3-183054
 | * Proposed TR Background Clause
 | * Sprint
 | * approved
 | * -
 | * -
 |
| * S3-183055
 | * Proposed TR Introduction Clause
 | * Sprint
 | * approved
 | * -
 | * -
 |
| * S3-183056
 | * Proposed Requirements, assumptions, and constraints Clause
 | * Sprint
 | * noted
 | * -
 | * -
 |
| * S3-183057
 | * Proposed Scope Clause
 | * Sprint
 | * revised
 | * -
 | * S3-183175
 |
| * S3-183058
 | * Draft TR 33.855
 | * Deutsche Telekom
 | * approved
 | * -
 | * -
 |
| * S3-183059
 | * LS on replay protection
 | * Ericsson
 | * approved
 | * -
 | * -
 |
| * S3-183060
 | * Draft TS 33.511
 | * Huawei
 | * approved
 | * -
 | * -
 |
| * S3-183061
 | * draft TS 33.512
 | * Deutsche Telekom
 | * approved
 | * -
 | * -
 |
| * S3-183062
 | * Draft TS 33.513
 | * Samsung
 | * approved
 | * -
 | * -
 |
| * S3-183063
 | * Draft TS 33.514
 | * NEC
 | * approved
 | * -
 | * -
 |
| * S3-183064
 | * LS Inter-PLMN security
 | * Nokia
 | * approved
 | * -
 | * -
 |
| * S3-183065
 | * agreements on initial NAS message security
 | * Qualcomm
 | * noted
 | * -
 | * -
 |
| * S3-183066
 | * LS on initial NAS security agreements
 | * Qualcomm
 | * approved
 | * -
 | * -
 |
| * S3-183067
 | * Draft TR 33.856
 | * Huawei
 | * approved
 | * -
 | * -
 |
| * S3-183068
 | * Draft TR 33.861
 | * Ericsson
 | * approved
 | * -
 | * -
 |
| * S3-183069
 | * Draft TR 33.807
 | * Huawei
 | * approved
 | * -
 | * -
 |
| * S3-183070
 | * Interworking - correcting keying material in HO request message (EPS to 5GS)
 | * Ericsson
 | * approved
 | * S3-183034
 | * -
 |
| * S3-183071
 | * Inteworking - reply LS on key update
 | * Ericsson
 | * approved
 | * S3-183033
 | * -
 |
| * S3-183072
 | * Corrections and additions in definitions and related clauses
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182954
 | * -
 |
| * S3-183073
 | * Reply to: LS on Transmission mechanism of SUCI in NAS procedure
 | * NEC
 | * approved
 | * -
 | * -
 |
| * S3-183074
 | * Reply to: Reply LS on Routing ID
 | * BT
 | * approved
 | * -
 | * -
 |
| * S3-183075
 | * NAS key refresh
 | * Ericsson
 | * approved
 | * S3-183026
 | * -
 |
| * S3-183076
 | * Acknowledging possibility of early calculation of EMSK
 | * Qualcomm Incorporated
 | * approved
 | * S3-182990
 | * -
 |
| * S3-183077
 | * Clarification to support of authentication methods
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182956
 | * -
 |
| * S3-183078
 | * Clarifications to clause 13.2.x
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182988
 | * -
 |
| * S3-183079
 | * Remove EN in clause 13.2.y.1
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182996
 | * -
 |
| * S3-183080
 | * Correction in step 2 of 13.2.y.2
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182998
 | * -
 |
| * S3-183081
 | * Corrections in 13.2.y.4 on N32-f context ID
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182999
 | * -
 |
| * S3-183082
 | * Handling of encrypted IEs on the N32 interface
 | * Deutsche Telekom AG
 | * approved
 | * S3-182821
 | * -
 |
| * S3-183083
 | * Preference of protection policies on the N32 interface
 | * Deutsche Telekom AG
 | * approved
 | * S3-182820
 | * -
 |
| * S3-183084
 | * pCR to S3-182700 regarding N32-f key hierarchy
 | * China Mobile
 | * approved
 | * S3-183002
 | * -
 |
| * S3-183085
 | * Clarification to N32 Procedure on insertion of decrypted values
 | * Ericsson
 | * noted
 | * S3-182974
 | * -
 |
| * S3-183086
 | * N32 related definitions
 | * Nokia, Nokia Shanghai Bell
 | * withdrawn
 | * -
 | * -
 |
| * S3-183087
 | * Editorial corrections on Authorization of NF service access
 | * Huawei, Hisilicon
 | * approved
 | * S3-182901
 | * -
 |
| * S3-183088
 | * Add discover procedure as a pre-requisite for obtaining access token
 | * Huawei, Hisilicon
 | * approved
 | * S3-182905
 | * -
 |
| * S3-183089
 | * Token caching
 | * Ericsson
 | * approved
 | * S3-182985
 | * -
 |
| * S3-183090
 | * NF instances in token claims
 | * Ericsson
 | * approved
 | * S3-182986
 | * -
 |
| * S3-183091
 | * Key Issue for fitting BEST into 5G system
 | * Alibaba (China) Group., Ltd.
 | * noted
 | * S3-182982
 | * -
 |
| * S3-183092
 | * Key Issue on secure communication between UE and enterprise application server
 | * Alibaba (China) Group., Ltd.
 | * revised
 | * S3-182983
 | * S3-183158
 |
| * S3-183093
 | * Key Issue Contents “Termination points of N32 security”
 | * Deutsche Telekom AG
 | * approved
 | * S3-182831
 | * -
 |
| * S3-183094
 | * Key Issue Contents “N32 error signalling”
 | * Deutsche Telekom AG
 | * approved
 | * S3-182832
 | * -
 |
| * S3-183095
 | * New Key Issue "Modifications by authorized intermediaries on N32"
 | * Deutsche Telekom AG
 | * approved
 | * S3-182833
 | * -
 |
| * S3-183096
 | * TLS and routing key issue
 | * Ericsson
 | * approved
 | * S3-182984
 | * -
 |
| * S3-183097
 | * Clarification to AUSF key derivation
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182955
 | * -
 |
| * S3-183098
 | * Alignment regarding KEY reference to 33.220
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182958
 | * -
 |
| * S3-183099
 | * Misleading text with reference regarding serving network name
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182959
 | * -
 |
| * S3-183100
 | * Update of EAP-AKA’ reference to make it compatible with 5G
 | * Ericsson
 | * noted
 | * S3-183039
 | * -
 |
| * S3-183101
 | * correction on the mobility from 5G to 4G
 | * Huawei, Hisilicon
 | * approved
 | * S3-182893
 | * -
 |
| * S3-183102
 | * Clarification on handover from EPS to 5GS
 | * Huawei, Hisilicon
 | * approved
 | * S3-182900
 | * -
 |
| * S3-183103
 | * Editorial corrections on the 5GS to EPS handover procedure
 | * Huawei, HiSilicon
 | * approved
 | * S3-182933
 | * -
 |
| * S3-183104
 | * Clarification for Target to Source container
 | * Huawei, HiSilicon
 | * approved
 | * S3-182934
 | * -
 |
| * S3-183105
 | * DRAFT LS on ResumeMAC-I Calculation for RRC Resume Request
 | * Huawei, Hisilicon
 | * withdrawn
 | * -
 | * -
 |
| * S3-183106
 | * UP security policy in NN-DC and MR-DC
 | * Huawei, Hisilicon, Qualcomm Incorporated, and Ericsson
 | * approved
 | * S3-182917
 | * -
 |
| * S3-183107
 | * Integrity protection of RRC-signalling
 | * NEC Corporation
 | * approved
 | * S3-182868
 | * -
 |
| * S3-183108
 | * Integrity protection of user data between the UE and the gNB
 | * NEC Corporation
 | * approved
 | * S3-182865
 | * -
 |
| * S3-183109
 | * Ciphering of RRC-signalling
 | * NEC Corporation
 | * approved
 | * S3-182867
 | * -
 |
| * S3-183110
 | * Ciphering of user data between the UE and the gNB.
 | * NEC Corporation
 | * approved
 | * S3-182863
 | * -
 |
| * S3-183111
 | * Security Assurance Requirement and Test for synchronization failure handling in the AMF
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182840
 | * -
 |
| * S3-183112
 | * Ciphering of NAS signalling message
 | * NEC Corporation, Deutsche Telekom AG
 | * approved
 | * S3-182876
 | * -
 |
| * S3-183113
 | * Integrity protection of NAS signalling messages
 | * NEC Corporation, Deutsche Telekom AG
 | * approved
 | * S3-182877
 | * -
 |
| * S3-183114
 | * Confidentiality protection of user data transported over N3 interface
 | * NEC Corporation, Samsung
 | * approved
 | * S3-182879
 | * -
 |
| * S3-183115
 | * Integrity protection of user data transported over N3 interface
 | * NEC Corporation, Samsung
 | * approved
 | * S3-182880
 | * -
 |
| * S3-183116
 | * Replay protection of user data transported over N3 interface
 | * NEC Corporation, Samsung
 | * approved
 | * S3-182881
 | * -
 |
| * S3-183117
 | * Resolving the SUPI from the SUCI based on the protection scheme used to generate the SUCI
 | * NEC Corporation
 | * approved
 | * S3-182882
 | * -
 |
| * S3-183118
 | * Storing authentication status of UE
 | * NEC Corporation
 | * approved
 | * S3-182883
 | * -
 |
| * S3-183119
 | * Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access
 | * Huawei, HiSilicon
 | * approved
 | * S3-182935
 | * -
 |
| * S3-183120
 | * Draft\_CR Corrections to Untrusted Non3GPP access clause
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-183015
 | * -
 |
| * S3-183121
 | * Update references
 | * Juniper Networks, Ericsson
 | * approved
 | * S3-182824
 | * -
 |
| * S3-183122
 | * Update NDS/IP scope with application layer crypto profiles
 | * Juniper Networks, Ericsson
 | * approved
 | * S3-182822
 | * -
 |
| * S3-183123
 | * Privacy - max. size of scheme-output for proprietary protection schemes
 | * Ericsson
 | * noted
 | * S3-182976
 | * -
 |
| * S3-183124
 | * skeleton of TS 33NEF
 | * ZTE Corporation
 | * approved
 | * S3-182850
 | * -
 |
| * S3-183125
 | * skeleton of KDF negotiation
 | * Huawei, Hisilicon
 | * approved
 | * S3-182898
 | * -
 |
| * S3-183126
 | * skeleton of URLLC Study
 | * Huawei, HiSilicon
 | * approved
 | * S3-182928
 | * -
 |
| * S3-183127
 | * Clarifications and corrections in clause 13.2.a
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-183001
 | * -
 |
| * S3-183128
 | * Security procedure when returns to E-UTRAN or NR from UTRAN
 | * Huawei, Hisilicon
 | * approved
 | * S3-182890
 | * -
 |
| * S3-183129
 | * Security procedure when returns to E-UTRAN or NR from UTRAN
 | * Huawei, Hisilicon
 | * approved
 | * S3-182891
 | * -
 |
| * S3-183130
 | * Proposed resolution of the editor’s note in the conclusion clause of TR 33.856
 | * Qualcomm Incorporated
 | * approved
 | * S3-182992
 | * -
 |
| * S3-183131
 | * Additional impacts on existing nodes and functionality for each solution
 | * Huawei, Hisilicon
 | * approved
 | * S3-182892
 | * -
 |
| * S3-183132
 | * New KI proposal for TR 33.861 on CIoT security - frequent small data transmissions for low complexity UEs
 | * InterDigital, Inc., T-Mobile USA
 | * approved
 | * S3-182805
 | * -
 |
| * S3-183133
 | * New key issue for integrity protection of small data
 | * Ericsson
 | * approved
 | * S3-183021
 | * -
 |
| * S3-183134
 | * New key issue for encryption of small data
 | * Ericsson
 | * approved
 | * S3-183022
 | * -
 |
| * S3-183135
 | * New Key Issue: Dealing with Malicious Applications on the UE
 | * KPN N.V.
 | * approved
 | * S3-183011
 | * -
 |
| * S3-183136
 | * Key Issue on gNB Protection from CIoT DoS attack
 | * Huawei, Hisilicon
 | * approved
 | * S3-182858
 | * -
 |
| * S3-183137
 | * scope of TR33807
 | * Huawei, Hisilicon
 | * approved
 | * S3-182916
 | * -
 |
| * S3-183138
 | * new requirement of 5G RG
 | * Huawei, Hisilicon
 | * approved
 | * S3-182907
 | * -
 |
| * S3-183139
 | * New key issue: FN-RG authentication and authorization
 | * Ericsson
 | * approved
 | * S3-182970
 | * -
 |
| * S3-183140
 | * new requirement in IPTV supported
 | * Huawei, Hisilicon
 | * withdrawn
 | * -
 | * -
 |
| * S3-183141
 | * New key issue: Transport security for the interfaces between W-5GAN and 5GC
 | * Ericsson
 | * approved
 | * S3-182971
 | * -
 |
| * S3-183142
 | * Privacy - LS on maximum output size of SUPI concealment schemes
 | * Ericsson
 | * approved
 | * S3-182977
 | * -
 |
| * S3-183143
 | * LS RRC Reestablishment during N2 handover
 | * Huawei
 | * approved
 | * -
 | * -
 |
| * S3-183144
 | * New key issue: Security for the interface between 5G-RG and W-5GAN
 | * Ericsson
 | * approved
 | * S3-182972
 | * -
 |
| * S3-183145
 | * Key Issue on Registration and NAS transport for trusted non-3GPP access
 | * Motorola Mobility, Lenovo
 | * approved
 | * S3-182938
 | * -
 |
| * S3-183146
 | * Solution for trusted access
 | * Motorola Mobility UK Ltd.
 | * approved
 | * S3-182940
 | * -
 |
| * S3-183147
 | * Key Issue on Access to 5GC from UEs that do not support NAS
 | * Motorola Mobility, Lenovo
 | * approved
 | * S3-182936
 | * -
 |
| * S3-183148
 | * Draft TR 33.815
 | * Sprint
 | * approved
 | * -
 | * -
 |
| * S3-183149
 | * PARLOS Key issue: Providing temperory security for unauthenticated UEs
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182844
 | * -
 |
| * S3-183150
 | * Support for Unauthenticated UEs access to RLOS using EPC
 | * Intel Corporation (UK) Ltd
 | * approved
 | * S3-182871
 | * -
 |
| * S3-183151
 | * PARLOS security solution
 | * Motorola Mobility, Lenovo
 | * approved
 | * S3-182932
 | * -
 |
| * S3-183152
 | * LTKUP: solution#5 evaluation against key issue #5
 | * Gemalto N.V.
 | * approved
 | * S3-182997
 | * -
 |
| * S3-183153
 | * Draft TR 33.834
 | * Vodafone
 | * approved
 | * -
 | * -
 |
| * S3-183154
 | * Key issue on AKMA architecture
 | * Ericsson
 | * approved
 | * S3-183032
 | * -
 |
| * S3-183155
 | * Key Issue on mutual authentication between UE and BSF
 | * Huawei, Hisilicon
 | * approved
 | * S3-182899
 | * -
 |
| * S3-183156
 | * AKMA - new KI authentication framework
 | * Ericsson
 | * approved
 | * S3-183031
 | * -
 |
| * S3-183157
 | * Draft TR 33.835
 | * China Mobile
 | * approved
 | * -
 | * -
 |
| * S3-183158
 | * Key Issue on secure communication between UE and enterprise application server
 | * Alibaba (China) Group., Ltd.
 | * approved
 | * S3-183092
 | * -
 |
| * S3-183159
 | * AKMA - new KI protecting privacy in control and data traffic
 | * Ericsson
 | * approved
 | * S3-183030
 | * -
 |
| * S3-183160
 | * New KI: Protection of AKMA architecture interfaces
 | * Ericsson
 | * approved
 | * S3-183038
 | * -
 |
| * S3-183161
 | * New KI: Key separation for AKMA AFs
 | * Ericsson
 | * approved
 | * S3-183016
 | * -
 |
| * S3-183162
 | * Discussion and pCR for decoupling secure procedure with specific protocol in AKMA
 | * China Mobile, KPN, LG electronics, Alibaba (China) Group., Ltd.
 | * approved
 | * S3-183007
 | * -
 |
| * S3-183163
 | * Candidate solution of introducing third party key to AKMA
 | * China Mobile
 | * approved
 | * S3-183008
 | * -
 |
| * S3-183164
 | * Reply LS on Clarifications on SUPI definition and NAI format
 | * IDEMIA
 | * noted
 | * -
 | * -
 |
| * S3-183165
 | * pCR to 33.841 - Addition of text for LTKUP impacts
 | * Vodafone GmbH
 | * approved
 | * S3-182964
 | * -
 |
| * S3-183166
 | * Clause 11: Desired performance aspects
 | * Ericsson
 | * approved
 | * S3-182979
 | * -
 |
| * S3-183167
 | * pCR to 33.841 - Update to requirements section
 | * Vodafone GmbH
 | * approved
 | * S3-182965
 | * -
 |
| * S3-183168
 | * LS on to RAN2/3 on the Impacts of increasing the MAC-I size
 | * Vodafone GmbH, AT&T
 | * approved
 | * S3-182962
 | * -
 |
| * S3-183169
 | * Draft TR 33.841
 | * Vodafone
 | * approved
 | * -
 | * -
 |
| * S3-183170
 | * Key issu-Avoiding AS security when application security enabled
 | * Nokia, Nokia Shanghai Bell
 | * approved
 | * S3-182843
 | * -
 |
| * S3-183171
 | * New key issue for security key refreshing
 | * Ericsson
 | * approved
 | * S3-183018
 | * -
 |
| * S3-183173
 | * Solution on Small Data Transfer for NAS Solution
 | * Huawei, Hisilicon
 | * approved
 | * S3-182895
 | * -
 |
| * S3-183174
 | * Output of evening session on initial NAS security
 | * NTT-Docomo
 | * noted
 | * -
 | * -
 |
| * S3-183175
 | * Proposed Scope Clause
 | * Sprint
 | * revised
 | * S3-183057
 | * S3-183177
 |
| * S3-183176
 | * New key issue for security key and authentication tag size
 | * Ericsson
 | * approved
 | * S3-183020
 | * -
 |
| * S3-183177
 | * Proposed Scope Clause
 | * Sprint
 | * approved
 | * S3-183175
 | * -
 |
| * S3-183178
 | * Adjusting the description of of the initial NAS protection method
 | * Qualcomm
 | * approved
 | * -
 | * -
 |
| * S3-183179
 | * Procedure to deal with draft CRs from this meeting
 | * WG Chair
 | * noted
 | * -
 | * -
 |

## Annex B: List of change requests

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Document | Title | Source | Spec | CR | Rev | Rel | Cat | WI | Decision |
| * S3-182826
 | * Alignment of AS layer handling of EPS to 5GS handover with N2 handover
 | * CATT
 | * 33.501
 | * -
 | * -
 | * Rel-15
 | * F
 | * 5GS\_Ph1-SEC
 | * withdrawn
 |
| * S3-182827
 | * Correction to Nudm\_UEAuthentication\_ResultConfirmation service
 | * CATT
 | * 33.501
 | * -
 | * -
 | * Rel-15
 | * F
 | * 5GS\_Ph1-SEC
 | * withdrawn
 |
| * S3-182841
 | * CR on Clarifictaions to Untrusted non-3GPP access clause
 | * Nokia, Nokia Shanghai Bell
 | * 33.501
 | * -
 | * -
 | * Rel-15
 | * F
 | * 5GS\_Ph1-SEC
 | * withdrawn
 |
| * S3-182921
 | * Editorial corrections on the 5GS to EPS handover procedure
 | * Huawei, HiSilicon
 | * 33.501
 | * -
 | * -
 | * Rel-15
 | * F
 | * 5GS\_Ph1-SEC
 | * withdrawn
 |
| * S3-182922
 | * Clarification for Target to Source container
 | * Huawei, HiSilicon
 | * 33.501
 | * -
 | * -
 | * Rel-15
 | * F
 | * 5GS\_Ph1-SEC
 | * withdrawn
 |
| * S3-182927
 | * Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access
 | * Huawei, HiSilicon
 | * 33.501
 | * -
 | * -
 | * Rel-15
 | * F
 | * 5GS\_Ph1-SEC
 | * withdrawn
 |

## Annex C: Lists of liaisons

### C1: Incoming liaison statements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document | Original | Title | From | Decision | Reply in |
| * S3-182809
 |  | * LS on Transmission mechanism of SUCI in NAS procedure
 | * C1-185663
 | * replied to
 | * S3-183073
 |
| * S3-182810
 |  | * LS on Clarifications on SUPI definition and NAI format
 | * C4-186573
 | * noted
 |  |
| * S3-182811
 |  | * Reply LS on AUSF/UDM instance selection and SUCI parameters
 | * C4-186606
 | * noted
 |  |
| * S3-182812
 |  | * LS on Key Update
 | * R2-1813403
 | * replied to
 | * S3-183033
 |
| * S3-182813
 |  | * LS on Routing ID
 | * S2-188870
 | * noted
 |  |
| * S3-182814
 |  | * Reply to CT4 LS on Nausf\_SoRProtection service
 | * S2-189035
 | * noted
 |  |
| * S3-182815
 |  | * LS reply to BBF Response to 3GPP SA2 liaison S2-183036 on ‘general status of work
 | * S2-189038
 | * noted
 |  |
| * S3-182816
 |  | * Reply LS on clarification on Restricted Operator Services
 | * S2-181407
 | * postponed
 |  |
| * S3-182817
 |  | * LS on devices behind 5G-RG accessing the 5GC
 | * S3i180377
 | * noted
 |  |
| * S3-182818
 |  | * LS on SG17 work item X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
 | * ITU-T SG17
 | * postponed
 |  |
| * S3-182819
 |  | * Reply LS on Routing ID
 | * CP-182238
 | * replied to
 | * S3-183074
 |
| * S3-182884
 |  | * Guidance on initial NAS message protection
 | * SP-180914
 | * replied to
 | * S3-183066
 |

### C2: Outgoing liaison statements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document | Title | To | Cc | reply to i/c LS |
| * S3-183059
 | * LS on replay protection
 | * RAN2
 | * RAN3
 |  |
| * S3-183064
 | * LS Inter-PLMN security
 | * CT4
 | * -
 |  |
| * S3-183066
 | * LS on initial NAS security agreements
 | * SA, SA2, CT1, RAN2, RAN3
 | * -
 | * S3-182884
 |
| * S3-183071
 | * Inteworking - reply LS on key update
 | * RAN2
 | * -
 | * S3-182812
 |
| * S3-183073
 | * Reply to: LS on Transmission mechanism of SUCI in NAS procedure
 | * CT1
 | * -
 | * S3-182809
 |
| * S3-183074
 | * Reply to: Reply LS on Routing ID
 | * CT1, SA2,CT
 | * CT4, CT6
 | * S3-182819
 |
| * S3-183142
 | * Privacy - LS on maximum output size of SUPI concealment schemes
 | * CT1, CT4
 | * RAN2, SA2
 | * -
 |
| * S3-183143
 | * LS RRC Reestablishment during N2 handover
 | * RAN2
 | * RAN3
 |  |
| * S3-183168
 | * LS on to RAN2/3 on the Impacts of increasing the MAC-I size
 | * RAN2, RAN3,CT1
 | * ETSI SAGE
 | * -
 |

## Annex D: List of draft Technical Specifications and Reports

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Spec | vers | Doc title |
| * S3-183058
 | * 33.855
 | * 1.2.0
 | * Draft TR 33.855
 |
| * S3-183060
 | * 33.511
 | * 0.2.0
 | * Draft TS 33.511
 |
| * S3-183061
 | * 33.512
 | * 0.3.0
 | * draft TS 33.512
 |
| * S3-183062
 | * 33.513
 | * 0.2.0
 | * Draft TS 33.513
 |
| * S3-183063
 | * 33.514
 | * 0.2.0
 | * Draft TS 33.514
 |
| * S3-183067
 | * 33.856
 | * 1.1.0
 | * Draft TR 33.856
 |
| * S3-183068
 | * 33.861
 | * 0.1.0
 | * Draft TR 33.861
 |
| * S3-183069
 | * 33.807
 | * 0.1.0
 | * Draft TR 33.807
 |
| * S3-183124
 | * 33.519
 | * 0.1.0
 | * skeleton of TS 33NEF
 |
| * S3-183125
 | * 33.808
 | * 0.1.0
 | * skeleton of KDF negotiation
 |
| * S3-183126
 | * 33.825
 | * 0.1.0
 | * skeleton of URLLC Study
 |
| * S3-183148
 | * 33.815
 | * 0.1.0
 | * Draft TR 33.815
 |
| * S3-183153
 | * 33.834
 | * 0.8.0
 | * Draft TR 33.834
 |
| * S3-183157
 | * 33.835
 | * 0.1.0
 | * Draft TR 33.835
 |
| * S3-183169
 | * 33.841
 | * 0.6.0
 | * Draft TR 33.841
 |

## Annex G: List of participants

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| TITLE | Family Name | Given Name | Employer Organization | Employer Category Code | Organization Represented | Organization Represented Category Code |
| Mr. | Arkko | Jari | Ericsson LM | ETSI | Ericsson LM | ETSI |
| Dr. | Arumugam | Sivabalan | NEC Europe Ltd | ETSI | NEC Europe Ltd | ETSI |
| Mr. | Ben Henda | Noamen | Ericsson LM | ETSI | Ericsson Japan K.K. | ARIB |
| 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. | Cichonski | Jeffrey | NIST | ATIS | NIST | ATIS |
| Mr. | Dolly | Martin | AT&T | ATIS | AT&T GNS Belgium SPRL | ETSI |
| Miss | Driscoll | Florence | NCSC | ETSI | NCSC | ETSI |
| Dr. | Escott | Adrian | Qualcomm CDMA Technologies | ETSI | Qualcomm CDMA Technologies | ETSI |
| Mr. | Evans | Tim P. | VODAFONE Group Plc | ETSI | Vodafone GmbH | ETSI |
| Mr. | Feng | Cheng | Datang Mobile Com. Equipment | CCSA | Datang Mobile Com. Equipment | CCSA |
| Mr. | Gamishev | Todor | Orange | ETSI | Orange | ETSI |
| Mrs. | Gao | Dan | Datang Linktester Technology | CCSA | Datang Linktester Technology | CCSA |
| Ms. | Guo | Shu | Apple Computer Trading Co. Ltd | CCSA | Apple Computer Trading Co. Ltd | CCSA |
| Mr. | Hu | Li | Huawei Technologies Co. Ltd. | ETSI | Huawei Technologies Co. Ltd. | ETSI |
| Miss | Huang | Xiaoting | China Mobile Com. Corporation | CCSA | China Mobile Com. Corporation | CCSA |
| Miss | Jerichow | Anja | Nokia Germany | ETSI | Nokia Germany | ETSI |
| Mrs. | Jia | Yunhe | DATANG TELECOM INTERNATIONAL | CCSA | DATANG TELECOM INTERNATIONAL | CCSA |
| Dr. | Jost | Christine | Ericsson LM | ETSI | Nanjing Ericsson Panda Com Ltd | CCSA |
| Dr. | Keesmaat | Iko | TNO | ETSI | KPN N.V. | ETSI |
| Dr. | Kim | Joonwoong | LG Electronics France | ETSI | LG Electronics Deutschland | ETSI |
| Mr. | Kohalmi | Steve | Juniper Networks | ETSI | Juniper Networks | ETSI |
| Mr. | Kolekar | Abhijeet | Intel Corporation (UK) Ltd | ETSI | Intel China Ltd. | CCSA |
| Mr. | Kujanen | Juha | Ericsson LM | ETSI | Ericsson India Private Limited | TSDSI |
| Dr. | Kunz | Andreas | Motorola Mobility Germany GmbH | ETSI | Motorola Mobility UK Ltd. | ETSI |
| Mr. | Leadbeater | Alex | BT plc | ETSI | BT plc | ETSI |
| Mr. | Li | He | Huawei Technologies Co. Ltd. | ETSI | Huawei Technologies Co. Ltd. | ETSI |
| Mrs. | Li | Jianwei | GOHIGH DATA NETWORKS TECH. | CCSA | GOHIGH DATA NETWORKS TECH. | CCSA |
| Ms. | Li | Yan | China Telecommunications | ETSI | China Telecomunication Corp. | CCSA |
| Dr. | Liu | Fuwen | China Mobile Com. Corporation | CCSA | China Mobile Com. Corporation | CCSA |
| Miss | Lu | Wei | Nokia Germany | ETSI | Nokia Shanghai Bell | CCSA |
| Mr. | Mellqvist | Anders | Sony Europe Limited | ETSI | Sony Europe Limited | ETSI |
| Dr. | Muhanna | Ahmad | Huawei Technologies Sweden AB | ETSI | HiSilicon Technologies Co. Ltd | CCSA |
| Mr. | Nair | Suresh | Nokia Germany | ETSI | Nokia Belgium | ETSI |
| Mr. | Normann | Henrik Andreas | Ericsson LM | ETSI | Ericsson GmbH, Eurolab | 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 |
| Dr. | Prasad | Anand | NEC Europe Ltd | ETSI | NEC Corporation | TTC |
| Mr. | Qi | Minpeng | China Mobile Com. Corporation | CCSA | China Mobile Com. Corporation | CCSA |
| Mr. | Rajadurai | Rajavelsamy | Samsung R&D Institute UK | ETSI | Samsung Electronics Co., Ltd | TTA |
| 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 |
| Dr. | Targali | Yousif | T-Mobile USA Inc. | ATIS | T-Mobile USA Inc. | ATIS |
| Mr. | Vujcic | Dragan | IDEMIA | ETSI | IDEMIA | ETSI |
| Dr. | Wang | Yong | HuaWei Technologies Co., Ltd | CCSA | HuaWei Technologies Co., Ltd | CCSA |
| Mr. | Whorlow | Colin | NCSC | ETSI | HOME OFFICE | ETSI |
| Mr. | Wong | Marcus | Huawei Tech.(UK) Co., Ltd | ETSI | Futurewei Technologies | ATIS |
| Mr. | Xie | Zhenhua | ZTE Corporation | ETSI | ZTE Corporation | ETSI |
| Mr. | Xu | Yang | Guangdong OPPO Mobile Telecom. | CCSA | Shenzhen YZF Network Technolog | CCSA |
| Mr. | Yoshizawa | Taka | NEC Europe Ltd | ETSI | NEC Corporation | TTC |
| Mr. | You | Shilin | ZTE Corporation | CCSA | ZTE Corporation | CCSA |
| Dr. | Yu | Xiaobo | Alibaba (China) Group., Ltd. | CCSA | Alibaba (China) Group., Ltd. | CCSA |
| Mrs. | Zhang | Rong | China Telecom Corporation Ltd. | CCSA | China Telecom Corporation Ltd. | CCSA |
| Mr. | Zhao | Xuwen | HiSilicon Technologies Co. Ltd | CCSA | HiSilicon Technologies Co. Ltd | CCSA |
| Mr. | Zhou | Wei | CATT | CCSA | CATT | CCSA |
| Dr. | Zugenmaier | Alf | NTT DOCOMO INC. | TTC | DOCOMO Communications Lab. | ETSI |

## Annex H: List of future meetings

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | Start date | End date (OP) | Town | Country | Reference |
| * SA3#72-LI
 | * 21/01/2019 09:00:00
 | * 24/01/2019 13:00:00
 | * Sophia Antipolis
 | * FR
 | * S3-ah-34081
 |
| * SA3#94
 | * 28/01/2019 09:00:00
 | * 01/02/2019 17:30:00
 | * India
 | * IN
 | * S3-94
 |
| * SA3#95
 | * 06/05/2019 09:00:00
 | * 10/05/2019 17:30:00
 | * Dubrovnik
 | * CR
 | * S3-95
 |
| * SA3-Ad-Hoc
 | * 24/06/2019 09:00:00
 | * 28/06/2019 17:00:00
 | * Sapporo
 | * JP
 | * S3-ah-40149
 |
| * SA3#96
 | * 26/08/2019 09:00:00
 | * 30/08/2019 17:30:00
 | * Wroclaw
 | * PL
 | * S3-96
 |
| * SA3-Ad-Hoc
 | * 14/10/2019 09:00:00
 | * 18/10/2019 17:30:00
 | * TBD
 |  | * S3-ah-40150
 |
| * SA3#97
 | * 18/11/2019 09:00:00
 | * 22/11/2019 17:30:00
 | * Sophia Antipolis
 | * FR
 | * S3-97
 |