Third Generation Partnership Project (3GPP™)

DRAFT Meeting Report
for
S3
meeting: 63

Chengdu, China, 11/04/2011 to 15/04/2011

1 Opening of the Meeting

The Chairman, Bengt Sahlin of Ericsson, opened the SA3#63 meeting in Chengdu, hosted by China Mobile and CATT, and gave the floor to Judy Zhu, of China Mobile, to give a welcoming speech and the practicalities.

The Chairman asked the group to hold a minute of silence for the victims of the recent earthquake and tsunami in Japan; a minute of silence was held. The Chairman also mentioned that the 3GPP ETWS system has successfully worked during the event, and it is believed to have saved many lives.

2 Approval of Agenda and Meeting Objectives

S3-110300 **Draft Agenda for THIS meeting**
Source: WG Chairman

Decision: The document was **approved**.

3 IPR Reminder

The attention of the delegates to the meeting of the SA3 Working 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.

4 Meeting Reports

S3-110302 **Report from LAST SA3 Ordinary meeting**
Source: WG Secretary

Discussion:

On action S3-62/3, MCC proposed creating an umbrella WI, including all current Rel-11 features as Building Blocks. This was agreed; the SA3 Chairman will propose this way forward to SA Plenary.

MCC will provide some written guidance on how to use this new WI.

Action S3-62/4 was successfully completed.

Decision: The document was **approved**.

S3-110301 **Report from LAST SA Plenary**
Source: WG Chairman

Decision: The document was **noted**.

S3-110345 **LS on Network Sharing**
Source: SP-110234

Discussion:

Vodafone asked whether the group thinks that there are existing features that might require corrections in the light of this LS; Vodafone also mentioned that one possible area could be backhaul security.

Nokia suggested that Rapporteurs should check whether their specifications are respecting the principle of network sharing; this was agreed.

ACTION: **check their specifications to see if there are any existing features where network sharing is not supported and report back**
(action on: Rapporteurs / due by:)

Decision: The document was **noted**.

Report from SA3-LI:

Alex Leadbeater, SA3-LI Chairman, gave an update on LI issues. The SA3 Guidelines were noted. The KMS Media Security LI solution was provided. 33.106 is to be re-worked; this is progressing. Some work on location reporting is being discussed. MDT was also of interest.

5 Items for early consideration

6 Reports and Liaisons from other Groups

IETF:

Some input on MIKEY-TICKET is available for the present meeting.

ETSI SAGE

There will be a new conference on ZUC; there is a claim that a new collision attack has been identified, but this has yet to be confirmed.

GSMA SG

Peter Howard gave an update on behalf of Charles Brookson; he mentioned that there is not an official Liaison Officer with GSMA as Charles Brookson is not attending SA3 anymore. A LO will have to be appointed. Peter Howard presented the information provided by Charles Brookson for the present meeting.

The last GSMA meeting was held in Dubai, at a joint session with the Fraud Forum, courtesy of Du, on 3-4th February 2011, our next meeting hosted by Nokia will be in Finland on May 17-18th.

At the last meeting issues discussed were:

- Mobile Malware Group (MMG) Updates as this is till a current issue, an interesting presentation was given on the situation in China,

- The GSMA Spam Reporting Service and how it could be used for Fraud Detection from Cloudmark, See http://gsmworld.com/newsroom/press-releases/2011/6032.htm

- Handset issues including updates on the secure wipe and counterfeit devices, Latest security issues, and signalling security.

- The latest Mobile Privacy Initiative,

http://gsmworld.com/newsroom/press-releases/2011/5992.htm

- The latest situation on algorithms, and evaluation status,

For those who have access to the GSMA Infocenter you can see the documents at:

https://infocentre.gsm.org/cgi-bin/grpdocsh.cgi?GrpID=SG&select_meet=3715

As usual, if anyone wishes to attend the GSMA SG please register for the next meeting or if you are not a member contact Charles Brookson or James Moran.

3GPP2:

No input.

OMA:

No input.

TCG:

Silke Holtmanns gave an update.

- MTM 2 Use cased approved for publication
- MTM 2 Requirements nearly complete
- MTM 2 Specification work ongoing
- TCG (MPWG) currently establishes a formal liaison with Global Platform for closer cooperation

7 Work Areas

7.1 IP Multimedia Subsystem (IMS)

7.1.1 Media Plane Security

7.1.2 Specification of Protection against Unsolicited Communications in IMS (SPUCI)

S3-110415 **SPUCI: Technical and Non-Technical Prevention Measures**
Source: Nokia Corporation, Nokia Siemens Networks

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

S3-110467 **Description of PUCI Function Communication**
Source: NEC Corporation

Discussion:

The first change was not agreed and the Editor's Note was left as it was.

In the second Editor's Note it was agreed to add that scores combining is FFS. Also, privacy indications on score are FFS.

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

S3-110468 **PUCI Description**
Source: NEC Corporation

Decision: The document was **withdrawn**.

S3-110550 **New version of SPUCI TR**
Source: NEC (Rapporteur)

Decision: The document was **agreed**.

7.1.3 Other Common IMS Issues

S3-110334 **Reply LS on Simultaneous registration of a single private identity from different UEs**
Source: S2-111153

Decision: The document was **noted**.

7.2 Network Domain Security

S3-110381 **[33.210] Clarification of algorithm names and DH group usage in IKEv2**
33.210 CR-39 (Rel-11) v11.1.0
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **agreed**.

S3-110382 **[33.210, rel-10] Correction of Iuh/Iurh security**
33.210 CR-40 (Rel-10) v10.2.0
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **agreed**.

S3-110383 **[33.210, rel-11] Correction of Iuh/Iurh security**
33.210 CR-41 (Rel-11) v11.1.0
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **agreed**.

S3-110379 **Correction of reference for key usage bit in TLS certificate and some editorials**
33.310 CR-51 (Rel-10) v10.2.0
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **agreed**.

S3-110380 **Correction on CRL distribution point for vendor root CA certificates**
33.310 CR-52 (Rel-10) v10.2.0
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **agreed**.

S3-110367 **Removal of mandatory support for HTTPS in CMP transport-R9**
33.310 CR-48 (Rel-9) v9.5.0
Source: Huawei, HiSilicon, Nokia Corporation, Nokia Siemens Networks

Decision: The document was **revised to S3-110567**.

S3-110567 **Removal of mandatory support for HTTPS in CMP transport-R9**
33.310 CR-48 rev 1 (Rel-9) v9.5.0
Source: Huawei, HiSilicon, Nokia Corporation, Nokia Siemens Networks

(Replaces S3-110367)

Decision: The document was **agreed**.

S3-110368 **Removal of mandatory support for HTTPS in CMP transport-R10**
33.310 CR-49 (Rel-10) v10.2.0
Source: Huawei, HiSilicon,Nokia Corporation, Nokia Siemens Networks

Decision: The document was **revised to S3-110568**.

S3-110568 **Removal of mandatory support for HTTPS in CMP transport-R10**
33.310 CR-49 rev 1 (Rel-10) v10.2.0
Source: Huawei, HiSilicon,Nokia Corporation, Nokia Siemens Networks

(Replaces S3-110368)

Decision: The document was **agreed**.

S3-110369 **CMPv2 message format**
33.310 CR-50 (Rel-11) v10.2.0
Source: Huawei, HiSilicon

Decision: The document was **noted**.

S3-110450 **NDS enhancement - SCEP option for Certificate Enrolment to support backhaul security and network elements in general (R11**
33.310 CR-CRNum (Rel-11) v10.2.0
Source: BT

Abstract:

To add SCEP option for Certificate Enrolment to support backhaul security and network elements in general (Release 11)

Discussion:

Nokia Siemens Networks and Deutsche Telekom would prefer to stick to only one protocol.

Decision: The document was **noted**.

7.3 UTRAN Network Access Security

7.4 GERAN Network Access Security

S3-110388 **Disc - A5/3 and A5/4 support in GSM**
Source: Orange

Decision: The document was **noted**.

S3-110389 CR - A5/3 and A5/4 support in GSM

43.020 CR-0027 (Rel-10) v9.1.0
Source: Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera

Discussion:

ALU supported mandating A5/3, but observed that it is too early for A5/4 mandatory support. Nokia had similar concerns and noted that Release 10 is frozen. Ericsson supported Nokia in this.

Ericsson observed that the problem stated by Orange is with legacy equipment, so mandating A5/3 for Release 10 would not address this problem. Orange proposed splitting the CR into support for A5/3 for Release 10 and A5/3-4 for Release 11; Ericsson replied this would not help for this problem.

Nokia Siemens Networks observed that 3G does not mandate encryption on the network side (LTE does). Nokia Siemens Networks expressed similar thoughts to Ericsson as per resolving the problem with legacy equipment.

Telecom Italia suggested that this CR would only help.

Nokia Siemens Networks suggested that there is a number of operators not co-signing this contribution, who are not interested in having this requirement mandated.

Vodafone suggested that the group should set a minimum security requirement, as it is one of the objectives of the WG.

Orange expressed concerns about security should this requirement not be mandated. Orange and Vodafone suggested that adding this requirement would help operators to enable A5/3-4 when necessary.

BT asked whether that also A5/1 should be prohibited to prevent bidding down attacks. Telecom Italia suggested this would be too soon.

Ericsson suggested this CR would only help greenfield operators.

Vodafone reiterated the proposal by Orange to split the CR into Rel-10 and 11. Nokia Siemens Networks suggested that this does not fall into the FASMO category. Vodafone observed that Nokia Siemens Networks would prefer not to mandate any algorithm on the network side; Nokia Siemens Networks replied that the concern is more about Release 10, being this frozen. BT suggested that the A5/1 attacks could be considered FASMO.

Huawei shared the concerns of Ericsson and Nokia Siemens Networks but also proposed recommending A5/3-4 for Release 10 and mandating them for subsequent releases. ALU suggested that Release 11 for A5/3 could be something acceptable. Vodafone objected to this, both for excluding A5/4 and Release 10.

Nokia Siemens Networks asked why A5/4 should be mandated if A5/3 can be used. Vodafone suggested that active attacks could be prevented.

NTT Docomo expressed surprise that the LS from GSMA in 388 dates back to 2007 and that the views of the operators have not been taken into account.

After some offline discussion, Orange proposed splitting the CR into Release 10 (A5/3 mandatory on the BSS) and 11 (introducing A5/4 support). Nokia proposed moving the CR in 389 to Release 11. Orange suggested that the CR not only provides tools for operators that are not currently concerned about attacks might experience attacks in the future, but also guidance to operators that might be unaware of the risks.

Decision: The document was **revised to S3-110553**.

S3-110553 CR - A5/3 support in GSM

43.020 CR-0027 rev 1 (Rel-10) v9.1.0
Source: Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera

(Replaces S3-110389)

Decision: The document was **agreed**.

S3-110554 **CR - A5/3 and A5/4 support in GSM**
43.020 CR-0028 (Rel-10) v9.1.0
Source: Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera

Decision: The document was **agreed**.

7.5 GAA

7.5.1 TS 33.223 GBA Push

7.5.2 TS 33.224 GBA Push Generic Layer

7.5.3 Other GAA Issues

S3-110502 **Security Enhancement for Usage of GBA from Browser**
Source: Ericsson, ST-Ericsson

Discussion:

Orange raised concerns about exposing the API. CMCC supported this concern.

Nokia recognized that the threat is valid, but the description may be incomplete.

Some further consideration is necessary.

Decision: The document was **noted**.

S3-110504 **Usage of GBA with the Web**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110503 **Security enhancements for usage of GBA from the browser**
Source: Nokia Corporation, Nokia Siemens Networks, China Mobile

Discussion:

Gemalto suggested UICC impact is not known; this was agreed.

Ericsson asked whether the need for normative work will be determined accordingly to the outcome of the informative study; this was confirmed.

Ericsson asked whether it should be specified the work is addressing javascript; Nokia replied that this is the most obvious way but there are other solutions that should be studied. It was agreed to rephrase the first two bullets to state that they address new scenarios. 'Study' was added to 'outline' and 'identify' first two bullets.

AT&T, Ericsson and ST-Ericsson supported the WI.

Decision: The document was **revised to S3-110551**.

S3-110551 **Security enhancements for usage of GBA from the browser**
Source: Nokia Corporation, Nokia Siemens Networks, China Mobile

(Replaces S3-110503)

Decision: The document was **approved**.

7.6 Multimedia Broadcast/Multicast Service (MBMS)

7.7 SAE/LTE Security

7.7.1 TS 33.401 Issues

S3-110341 **LS on excessive updates of NAS security context**
Source: C6-110184

Decision: The document was **replied to in S3-110529**.

S3-110529 **Reply to: LS on excessive updates of NAS security context**
Source: Ericsson

Decision: The document was **approved**.

S3-110359 **Discussion on excessive update of NAS Security Context in the LS C6-110184**
Source: Huawei, HiSilicon

Decision: The document was **noted**.

S3-110452 **Memory stress due to excessive updates of NAS security context**
Source: AT&T, Ericsson, Gemalto, Samsung, ST-Ericsson, Verizon Wireless

Discussion:

ALU suggested that plastic roaming is not used; Nokia Siemens Networks recognized that this is not a strong reason to host the NAS security context on the UICC, however, as mentioned on the LS, the problem persists even if the non-volatile memory of the ME is considered as an alternative.

ALU asked whether deregistration is a frequent event. Vodafone suggested that the scenario on the LS is much more frequent than deregistration. Nokia suggested that according to analysis, deregistration could occur up to ten times per day under certain scenarios.

Qualcomm agreed with ALU and suggested that plastic roaming is not that common anymore. Qualcomm added that the paper considers only one state transition (EMM-DEREGISTERED, EMM-REGISTERED) but more states should be considered. Qualcomm also suggested that terminology should be aligned; Ericsson agreed and suggested that the modified 453 CR sent on the exploder (S3-110525) gives clarity on that perspective.

Decision: The document was **noted**.

S3-110453 **33.401 CR R8 Modification of security context storage rate**
33.401 CR-457 (Rel-8) v8.7.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola

Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

Decision: The document was **revised to S3-110514**.

S3-110514 **33.401 CR R8 Modification of security context storage rate**
33.401 CR-457 rev 1 (Rel-8) v8.7.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110453)

Decision: The document was **revised to S3-110525**.

S3-110525 **33.401 CR R8 Modification of security context storage rate**
33.401 CR-457 rev 2 (Rel-8) v8.7.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110514)

Decision: The document was **revised to S3-110526**.

S3-110526 **33.401 CR R8 Modification of security context storage rate**
33.401 CR-457 rev 3 (Rel-8) v8.7.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110525)

Discussion:

NTT Docomo suggested that the atomicity of the operation should be taken care of; SA3 suggested that the CR attempts to be sufficiently high-level so as not to contradict the CT1 text.

Decision: The document was **agreed**.

S3-110454 **33.401 CR R9 Modification of security context storage rate**
33.401 CR-458 (Rel-9) v9.6.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

Decision: The document was **revised to S3-110515**.

S3-110515 **33.401 CR R9 Modification of security context storage rate**
33.401 CR-458 rev 1 (Rel-9) v9.6.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110454)

Decision: The document was **revised to S3-110527**.

S3-110527 **33.401 CR R9 Modification of security context storage rate**
33.401 CR-458 rev 2 (Rel-9) v9.6.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110515)

Decision: The document was **agreed**.

S3-110455 **33.401 CR R10 Modification of security context storage rate**
33.401 CR-459 (Rel-10) v10.0.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

Decision: The document was **revised to S3-110516**.

S3-110516 **33.401 CR R10 Modification of security context storage rate**
33.401 CR-459 rev 1 (Rel-10) v10.0.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110455)

Decision: The document was **revised to S3-110528**.

S3-110528 **33.401 CR R10 Modification of security context storage rate**
33.401 CR-459 rev 2 (Rel-10) v10.0.0
Source: Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation

(Replaces S3-110516)

Decision: The document was **agreed**.

S3-110506 **Modification of security context storage rate on the USIM**
33.102 CR-CRNum (Rel-11) v10.0.0
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

Telecom Italia asked why such a change should be applied to address an issue that has not occurred; Nokia Siemens Networks replied that HSPA might bring similar effects to the LTE case for 3G terminals.

It was agreed that Nokia will chair the email discussion on the proposed draft CR, to understand whether this change is considered justified and welcome by the WG. The email discussion will end on June17 at the latest.

Decision: The document was **sent for email discussion**.

S3-110497 **EPS algorithm negotiation during UTRAN to E-UTRAN handover**
33.401 CR-428 (Rel-11) v9.6.0
Source: NEC Corporation

Abstract:

Closing chapter on I-RAT handover algorithm negotiation by adding text agreed in SA3#62.

Discussion:

Ericsson supported the idea and proposed a rewording; Vodafone supported the need for some rewording.

Vodafone suggested that the Note is rather long and mentioned that one solution could be to move the content in an informative Annex.

Nokia Siemens Networks supported the comments but would prefer shortening the Note rather than informative annex.

Qualcomm agreed that a simple Note is enough and the solution need not be illustrated.

Decision: The document was **revised to S3-110530**.

S3-110530 **EPS algorithm negotiation during UTRAN to E-UTRAN handover**
33.401 CR-428 rev 1 (Rel-11) v10.0.0
Source: NEC Corporation

(Replaces S3-110497)

Decision: The document was **agreed**.

7.7.2 TS 33.402 Issues

S3-110480 **Handling of maximum number of IKEv2 SAs**
Source: Ericsson, ST-Ericsson

Discussion:

CMCC disagreed with proposals 2-3. Ericsson suggested asking SA2 and CT1 on whether the non-security-related reasons justify the proposed CRs and whether there are further solution proposals by these WG's.

Orange suggested that a single given APN is considered should be made clear on the LS; Ericsson replied that the specifications mention also the case of multiple APNs.

Decision: The document was **noted**.

S3-110531 **LS on Handling of maximum number of IKEv2 Sas**
Source: Ericsson

Decision: The document was **approved**.

S3-110481 **33.402 CR (R10): Removal of maximum number of IKEv2 SA limit**
33.402 CR-96 (Rel-10) v10.0.0
Source: Ericsson, ST-Ericsson

Decision: The document was **postponed to the next meeting**.

S3-110482 **33.402 CR (R9): Removal of maximum number of IKEv2 SA limit**
33.402 CR-97 (Rel-9) v9.6.0
Source: Ericsson, ST-Ericsson

Decision: The document was **postponed to the next meeting**.

S3-110483 **33.234 CR (R10): Removal of maximum number of IKEv2 SA limit**
33.234 CR-109 (Rel-10) v10.0.0
Source: Ericsson, ST-Ericsson

Decision: The document was **postponed to the next meeting**.

S3-110484 **33.234 CR (R9): Removal of maximum number of IKEv2 SA limit**
33.234 CR-110 (Rel-9) v9.2.0
Source: Ericsson, ST-Ericsson

Decision: The document was **postponed to the next meeting**.

7.7.3 Relay Node Security

S3-110321 **LS reply on OAM architecture aspects for RNs (S5-110067 / R3-102541)**
Source: S5-110546

Decision: The document was **noted**.

S3-110329 **Reply LS on OAM architecture aspects for RNs**
Source: R3-110970

Decision: The document was **noted**.

S3-110326 **Reply LS on Relay Node OAM System Discovery**
Source: R3-110968

Decision: The document was **noted**.

S3-110342 **LS on additional considerations of Relay Nodes in the LTE-Advanced material for Rec. ITU-R M.[IMT.RSPEC] to be submitted to ITU-R WP5D#10 (6-13 April, 2011)**
Source: RP-110006

Decision: The document was **noted**.

S3-110330 **Reply LS on Security for LTE relay nodes**
Source: R3-111034

Decision: The document was **noted**.

S3-110520 **Proposed merger of S3-110396, 420, 451 Corrections to communication between MME and DeNB for relay nodes**

33.401 CR-450 rev 1 (Rel-10) v10.0.0
Source: Nokia Siemens Networks

Discussion:

ZTE supported the contribution. Orange suggested in 451 there was a sentence which is missing from the current proposal; Nokia Siemens Networks suggested that this is covered by step A2.

Ericsson suggested the fact that the MME informs the DeNB that the destination is the RN should be clear and a sentence should be added on this; Qualcomm supported this; this was agreed.

Decision: The document was **revised to S3-110533**.

S3-110533 **Corrections to communication between MME and DeNB for relay nodes**

33.401 CR-460 (Rel-10) v10.0.0
Source: Nokia Siemens Networks, China Mobile, Gemalto, NTT Docomo, ZTE

(Replaces S3-110520)

Decision: The document was **agreed**.

S3-110396 **Corrections to communication between MME and DeNB for relay nodes**

33.401 CR-450 (Rel-10) v10.0.0
Source: Nokia Siemens Networks, China Mobile, Gemalto

Decision: The document was **merged in 520**.

S3-110420 **Correction of the RN attach procedure**

33.401 CR-441 (Rel-10) v10.0.0
Source: ZTE Corporation

Decision: The document was **merged in 520**.

S3-110451 **Alignment of RN security with RAN2/3 decision given in LS S3-110330 (R3-111034)**

33.401 v10.0.0
Source: NTT docomo

Abstract:

RAN3 informed SA3 of their decision not to include an additional information element in S1 INITIAL CONTEXT SETUP message. This contribution provides the aligned security handling which provides the same security.

Decision: The document was **merged in 520**.

S3-110311 **Corrective text for undefined wording - autonomous validation of RN platform**

33.401 CR-440 (Rel-10) v10.0.0
Source: InterDigital, China Mobile, Nokia Siemens Networks

Decision: The document was **revised to S3-110534**.

S3-110534 **Corrective text for undefined wording - autonomous validation of RN platform**
33.401 CR-440 rev 1 (Rel-10) v10.0.0
Source: InterDigital, China Mobile, Nokia Siemens Networks

(Replaces S3-110311)

Decision: The document was **agreed**.

S3-110357 **Algorithm negotiation on Un interface**
Source: Huawei, HiSilicon

Decision: The document was **noted**.

S3-110358 **CR-Algorithm negotiation on Un interface**
33.401 CR-447 (Rel-10) v10.0.0
Source: Huawei, HiSilicon

Discussion:

Nokia Siemens Networks pointed out that RAN2 is addressing the issue in a different manner.

It was suggested that this is covered in other specifications; an offline check will be made.

After the check, the document was withdrawn.

Decision: The document was **withdrawn**.

S3-110395 **Resolution of Editor's Notes for PDPC integrity for Relay Nodes**
33.401 CR-449 (Rel-10) v10.0.0
Source: Nokia Siemens Networks

Discussion:

Two editorial changes were agreed.

It was also agreed that an example taken from S3-110421 will be added.

Decision: The document was **revised to S3-110535**.

S3-110535 **Resolution of Editor's Notes for PDPC integrity for Relay Nodes**
33.401 CR-449 rev 1 (Rel-10) v10.0.0
Source: Nokia Siemens Networks

(Replaces S3-110395)

Decision: The document was **agreed**.

S3-110421 **Supplemented description on how to handle the integrity verification failed message**
33.401 CR-442 (Rel-10) v10.0.0
Source: ZTE Corporation

Discussion:

A sentence from the contribution was agreed to be added in S3-110535.

Decision: The document was **noted**.

S3-110518 **Comments on S3-110421 Supplemented description on how to handle the integrity verification failed message**

Source: Nokia Siemens Networks

Decision: The document was **noted**.

S3-110351 **DISC-Analysis on binding of UICC and RN**

Source: Huawei, HiSilicon

Decision: The document was **noted**.

S3-110352 **CR-Detailed binding of RN and UICC**

33.401 CR-444 (Rel-10) v10.0.0

Source: Huawei, HiSilicon

Discussion:

Qualcomm suggested there are multiple ways of achieving this and there should not be any need to specify it.

Nokia Siemens Networks suggested any related changes would belong to D.2.3.

Decision: The document was **revised to S3-110536**.

S3-110536 **CR-Detailed binding of RN and UICC**

33.401 CR-444 rev 1 (Rel-10) v10.0.0

Source: Huawei, HiSilicon

(Replaces S3-110352)

Decision: The document was **agreed**.

S3-110397 **Specification of secure channel profiles and certificates used for Relay nodes (RNs) and UICC (USIM-RN)**

33.401 CR-451 (Rel-10) v10.0.0

Source: Nokia Siemens Networks

Decision: The document was **revised to S3-110537**.

S3-110537 **Specification of secure channel profiles and certificates used for Relay nodes (RNs) and UICC (USIM-RN)**

33.401 CR-451 rev 1 (Rel-10) v10.0.0

Source: Nokia Siemens Networks

(Replaces S3-110397)

Decision: The document was **agreed**.

S3-110400 **Correction on communication outside secure channel for Relay Node security procedures**
33.401 CR-454 (Rel-10) v10.0.0
Source: China Mobile, Gemalto, InterDigital Communications, Nokia Siemens Networks, Sagem-Orga

Discussion:

It was decided to remove "as a general rule".

Gemalto clarified that as the secure channel is established between RN and RN-USIM it is correct to refer to it. Nokia Siemens Networks proposed a rewording which was agreed.

Decision: The document was **revised to S3-110538**.

S3-110538 **Correction on communication outside secure channel for Relay Node security procedures**
33.401 CR-454 rev 1 (Rel-10) v10.0.0
Source: China Mobile, Gemalto, InterDigital Communications, Nokia Siemens Networks, Sagem-Orga

(Replaces S3-110400)

Decision: The document was **agreed**.

S3-110378 **Clarification of certificate and subscription handling**
33.401 CR-448 (Rel-10) v10.0.0
Source: China Mobile,Nokia Siemens Networks, Nokia Corporation

Discussion:

Deutsche Telekom suggested that the RN certificate is not invalidated, it is the UICC to be invalidated.

Decision: The document was **revised to S3-110539**.

S3-110539 **Clarification of certificate and subscription handling**
33.401 CR-448 rev 1 (Rel-10) v10.0.0
Source: China Mobile,Nokia Siemens Networks, Nokia Corporation

(Replaces S3-110378)

Decision: The document was **agreed**.

S3-110508 **RN certificate handling simplification**
33.401 CR-456 (Rel-10) v10.0.0
Source: NTT docomo

Abstract:

Annex D calls for UICC certificate validation against a CRL in the RN. However, both the format of the CRL and the protocol for fetching the CRL in step E.3 are not defined. The certificate check of the UICC can be omitted by ensuring IMSIs in use by revoked UICC are barred in the HSS.

Discussion:

It was agreed that the attack is valid.

It was discussed whether the attack is relevant.

Concerning the impersonation attack discussion; NTT Docomo suggested that the RN CRL, if the network is controlled by the attacker, will not be updated correctly.

It was decided to hold an email discussion on the subject.

Decision: The document was **postponed to the next meeting**.

S3-110521 **Comments on S3-110508 RN certificate handling simplification**
Source: Nokia Siemens Networks

Decision: The document was **noted**.

S3-110540 **Attack description concerning CRL handling in RN solution**
Source: NTT Docomo

Decision: The document was **noted**.

S3-110442 **Replacing S3-110422_Clarification of the secure connection between RN and OAM server**
33.401 CR-443 (Rel-10) v10.0.0
Source: ZTE Corporation

Decision: The document was **postponed to the next meeting**.

S3-110519 **Comments by Nokia Siemens Networks on S3-110442 Clarification of the secure connection between RN and OAM server**
Source: Nokia Siemens Networks

Discussion:

Vodafone suggested that all three types of protection might be necessary; additionally deleting the part in 5.3.2, then there would be no contradiction more in general. Nokia Siemens Networks pointed at the third paragraph in 13.

Vodafone suggested that there appear to be different interpretations of 33.401.

Deutsche Telekom suggested that secure protocols would be necessary; BT asked how this would be integrated with TR-069; Nokia Siemens Networks suggested that TR-069 is limited to HeNB. Juniper supported the Nokia Siemens Networks suggestion that additional protection would be necessary.

Nokia Siemens Networks asked whether companies would prefer e2e mandatory or optional: Vodafone suggested SA5 should be consulted on this. Nokia Siemens Networks suggested this question is about the requirement, not the implementation itself. Vodafone could not express an opinion at this meeting on this issue.

It was decided that further discussion and contributions on the subject are necessary and a decision will be taken at the next meeting.

There will not be a formal email discussion but communications between interested parties is encouraged.

Decision: The document was **noted**.

S3-110419 **Security handling for UE handover from Relay**
Source: Huawei, HiSilicon

Decision: The document was **noted**.

S3-110418 CR-Security handling for relay related UE handover

33.401 CR-446 (Rel-10) v10.0.0
Source: Huawei, HiSilicon

Discussion:

Ericsson asked what would be the gain in modifying the Rel-8 derivation method. Nokia Siemens Networks suggested that their understanding of the gain would be to achieve one-hop forward security, where currently Rel-8 offers two hop forward security.

Deutsche Telekom asked for further study before agreeing to such a change as the security gain seems to be rather low.

There was not enough support for the change.

Decision: The document was **noted**.

S3-110353 DISC-Clarification on initial attach procedure for PSK case

Source: Huawei, HiSilicon

Decision: The document was **noted**.

S3-110354 CR-Clarification on initial attach procedure for PSK case

33.401 CR-445 (Rel-10) v10.0.0
Source: Huawei, HiSilicon

Discussion:

Some alignments with comments from Ericsson and Nokia Siemens Networks have to be incorporated, and the baselines must be aligned.

Decision: The document was **revised to S3-110541**.

S3-110541 CR-Clarification on initial attach procedure for PSK case

33.401 CR-445 rev 1 (Rel-10) v10.0.0
Source: Huawei, HiSilicon

(Replaces S3-110354)

Decision: The document was **agreed**.

S3-110398 Resolution of Editor's Notes for Relay Node security procedures

33.401 CR-452 (Rel-10) v10.0.0
Source: Nokia Siemens Networks, China Mobile

Discussion:

The stage 3 references were agreed to be removed.

Decision: The document was **revised to S3-110542**.

S3-110542 **Resolution of Editor's Notes for Relay Node security procedures**
33.401 CR-452 rev 1 (Rel-10) v10.0.0
Source: Nokia Siemens Networks, China Mobile

(Replaces S3-110398)

Decision: The document was **agreed**.

S3-110399 **Corrections and Clarifications for Relay Node security procedures**
33.401 CR-453 (Rel-10) v10.0.0
Source: Nokia Siemens Networks, Gemalto

Discussion:

It was agreed to remove the CRL-related changes.

Decision: The document was **revised to S3-110543**.

S3-110543 **Corrections and Clarifications for Relay Node security procedures**
33.401 CR-453 rev 1 (Rel-10) v10.0.0
Source: Nokia Siemens Networks, Gemalto

(Replaces S3-110399)

Decision: The document was **agreed**.

7.7.4 EEA3 and EIA3 Issues

7.7.5 Other SAE/LTE Security Issues

S3-110333 **LS on partial success of Write Replace Warning Request for ETWS**
Source: R3-111084

Decision: The document was **noted**.

S3-110465 **draft LS on Security context mismatch in UMTS and GSM**
Source: Ericsson, ST-Ericsson

Decision: The document was **revised to S3-110544**.

S3-110544 **LS on Security context mismatch in UMTS and GSM**
Source: Ericsson, ST-Ericsson

(Replaces S3-110465)

Decision: The document was **approved**.

7.8 Security Aspects of Home (e)NodeB

S3-110305 **H(e)NB. Security of direct interfaces**
Source: Alcatel-Lucent, Alcatel-Lucent Shanghai Bell

Abstract:

SA3 is tasked with defining security of direct interfaces for H(e)NB in the Rel-11. This paper presents a view of different solutions for establishing of security, when and where it is required, for such interfaces.

Decision: The document was **noted**.

S3-110523 **Comment on'H(e)NB. Security of direct interfaces' (S3-110305)**
Source: Nokia Siemens Networks

Decision: The document was **noted**.

7.8.1 TS 33.320 Issues

S3-110370 **Security of direct interface between H(e)NBs**
Source: Huawei, HiSilicon

Discussion:

Vodafone suggested that it should be looked into whether authorization could be combined on either of the solutions. Vodafone added that the authorization requirements should be added. Qualcomm clarified that there are two different authorizations under discussion; Vodafone confirmed this understanding. These authorisations are for (1) establishment of direct link, and (2) allowing handover for certain UEs. Huawei, Qualcomm, NSN and Ericsson stated that authorisation for (2) is handled by RAN.

It was agreed to study only the authorization of the direct link. This was agreed to be considered as a requirement.

Samsung asked what would be the reason to study authentication; Huawei replied that this could be beneficial. Samsung suggested that IPsec should be mandatory.

ALU observed that the complexity is not correclty reflected in the comparison table (e.g. RA is not taken into account).

Orange would be reluctant to accept proposal 1 as there should always be some form of protection, as for X2.

Vodafone suggested that IPsec should be mandated on the Iurh as for the Iuh interface. China Mobile supported optional protection.

It was agreed that IPsec is mandatory to support (implement) for Iurh.

Decision: The document was **noted**.

S3-110469 **Security for direct interfaces between H(e)NBs**
33.320 CR-58 rev 1 (Rel-11) v11.1.0
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

Orange raised concerns working in tunnel mode for e2e and would prefer transport mode. Contributions are invited for the next meeting.

Orange raised a concern about network sharing, relating to the LS received by SA Plenary; this must be checked.

Samsung was confused as the contribution states IKEv2 is mandatory but IPsec is optional; Nokia Siemens Networks stated that the situation is similar to the macro eNB backhaul case.

It was decided to postpone the CR to the next meeting.

Decision: The document was **postponed to the next meeting**.

S3-110307 **A way forward for the treatment of the newly discovered vulnerability due to undefined H(e)NB Identity binding to H(e)NB-GW**
Source: Alcatel-Lucent, AT&T, Vodafone, Alcatel-Lucent Shanghai Bell

Abstract:

This paper presents a way forward for the treatment of the newly discovered vulnerability with the current security architecture of H(e)NB. It proposes that the described vulnerability be shared with 3GPP architecture working groups (RAN3 and SA2) in order to decide for appropriate changes in the H(e)NB architecture.

Discussion:

NEC had difficulties in understanding the description of the attack; Qualcomm pointed out it would be important to clearly depict the attack in a possible LS to other groups.

Vodafone suggested a solution to address the attack would be welcome, taking advantage of the access control mechanisms, should the solution prove to be efficient.

It was agreed to inform the interested WGs on the attack, via an LS - the groups will be asked to advise on the complexity and cost of the solution.

NTT Docomo would like to study other potential attacks as well.

Decision: The document was **noted**.

S3-110393 **DRAFT LS on CSG security for H(e)NB**
Source: Alcatel-Lucent, Alcatel-Lucent Shanghai Bell

Abstract:

This contribution presents draft LS on CSG security for H(e)NB.

Decision: The document was **revised to S3-110545**.

S3-110545 **LS on CSG security for H(e)NB**
Source: Alcatel-Lucent, Alcatel-Lucent Shanghai Bell

(Replaces S3-110393)

Decision: The document was **approved**.

S3-110384 **Security mechanism for H(e)NB no-IPsec usage option**
Source: Samsung

Decision: The document was **noted**.

S3-110385 **Security mechanism for H(e)NB no-IPsec usage option [Rel-9]**
33.320 CR-67 (Rel-9) v9.5.0
Source: Samsung

Discussion:

It was observed that some rewording should be performed to add clarity.

BT asked how would this functionality be switched on again, if switched off.

It was agreed to change "it was specified" to "it was mentioned".

Decision: The document was **revised to S3-110547**.

S3-110446 **HeNB security**
Source: China Mobile

Decision: The document was **noted**.

S3-110547 **Security mechanism for H(e)NB no-IPsec usage option [Rel-9]**
33.320 CR-67 rev 1 (Rel-9) v9.5.0
Source: Samsung

(Replaces S3-110385)

Decision: The document was **agreed**.

S3-110386 **Security mechanism for H(e)NB no-IPsec usage option [Rel-10]**
33.320 CR-66 (Rel-11) v10.2.0
Source: Samsung

Decision: The document was **revised to S3-110548**.

S3-110387 **Security mechanism for H(e)NB no-IPsec usage option [Rel-11]**
33.320 CR-67 (Rel-11) v11.1.0
Source: Samsung

Decision: The document was **revised to S3-110549**.

S3-110548 **Security mechanism for H(e)NB no-IPsec usage option [Rel-10]**
33.320 CR-66 rev 1 (Rel-10) v10.2.0
Source: Samsung

(Replaces S3-110386)

Decision: The document was **agreed**.

S3-110549 **Security mechanism for H(e)NB no-IPsec usage option [Rel-11]**
33.320 CR-67 rev 1 (Rel-11) v11.1.0
Source: Samsung

(Replaces S3-110387)

Decision: The document was **agreed**.

S3-110563 **LS on Security mechanism for H(e)NB no-IPsec usage option**
Source: CMCC

Decision: The document was **approved**.

S3-110390 **H(e)NB-LGW Remote IP Address Assignment [Rel-10]**
33.320 CR-70 (Rel-10) v10.2.0
Source: Samsung, Qualcomm

Discussion:

Nokia Siemens Networks would prefer to have an RFC reference.

Further clarification and solutions are invited.

Decision: The document was **noted**.

S3-110391 **H(e)NB-LGW Remote IP Address Assignment [Rel-11]**
33.320 CR-71 (Rel-11) v11.1.0
Source: Samsung, Qualcomm

Decision: The document was **noted**.

S3-110312 **Removal of Hosting Party Authentication, R9**
33.320 CR-62 (Rel-9) v9.4.0
Source: Qualcomm Incorporated

Abstract:

33.320 currently describes the use of hosting party authentication. However, CT6 have recently agreed a work item to define a new UICC application for HPMs (see C6-110088, C6-100634/S3-100157, as well as S1-110185). Because this application is only being developed within Release 11, there will be no support for hosting party authentication in earlier releases.

Discussion:

Telecom Italia did not support the proposal as there are no security reasons; Qualcomm pointed out that CT6 have listed several non-security related reasons.

Huawei and Gemalto did not support the contribution.

It was agreed to send an LS to CT6, pointing out that any potential work should be backwards compatible.

Decision: The document was **noted**.

S3-110313 **Removal of Hosting Party Authentication, R10**
33.320 CR-63 (Rel-10) v10.1.0
Source: Qualcomm Incorporated

Abstract:

33.320 currently describes the use of hosting party authentication. However, CT6 have recently agreed a work item to define a new UICC application for HPMs (see C6-110088, C6-100634/S3-100157, as well as S1-110185). Because this

application is only being developed within Release 11, there will be no support for hosting party authentication in earlier releases.

Decision: The document was **noted**.

S3-110546 **LS on backwards compatibility of HPIM**
Source: Qualcomm Incorporated

Decision: The document was **approved**.

S3-110314 **Location Verification Correction, R9**
33.320 CR-64 (Rel-9) v9.4.0
Source: Qualcomm Incorporated

Abstract:

Inconsistency between SA3 and RAN3 on network nodes performing location verification. 25.467 states clearly: 6.1.2.1General During location verification, the HNB reports its location information to the HMS. There is no mention of the HNB-GW.

Discussion:

Withdrawn after offline discussions during the meeting.

Decision: The document was **withdrawn**.

S3-110315 **Location Verification Correction, R10**
33.320 CR-65 (Rel-10) v10.1.0
Source: Qualcomm Incorporated

Abstract:

Inconsistency between SA3 and RAN3 on network nodes performing location verification. 25.467 states clearly: 6.1.2.1General During location verification, the HNB reports its location information to the HMS. There is no mention of the HNB-GW.

Decision: The document was **withdrawn**.

S3-110316 **Location Verification Correction, R11**
33.320 CR-66 (Rel-11) v11.0.0
Source: Qualcomm Incorporated

Abstract:

Inconsistency between SA3 and RAN3 on network nodes performing location verification. 25.467 states clearly: 6.1.2.1General During location verification, the HNB reports its location information to the HMS. There is no mention of the HNB-GW.

Decision: The document was **withdrawn**.

7.8.2 TR 33.820 Issues

7.9 Security Aspects related to System Improvements for Machine-Type Communication (SIMTC)

S3-110343 **Reply LS on MTC Planning and Prioritization**
Source: SP-110218

Decision: The document was **noted**.

S3-110392 **Update of SIMTC WID**
Source: Samsung

Discussion:

BT asked how the coordination with other standards bodies on gateways would be done. This will be discussed under the contribution in S3-110479.

CMCC pointed out the LS does not call the security part a BB but a Feature; there was some discussion on the terminology of primary/secondary responsibility; ALU asked to remove primary/secondary; MCC clarified these terms do not refer to priority, but leadership.

The text in 4 was agreed with a change of "assessment" to "assessor".

Decision: The document was **revised to S3-110555**.

S3-110555 **Update of SIMTC WID**
Source: Samsung

(Replaces S3-110392)

Decision: The document was **approved**.

S3-110417 **Analysis of MTC Planning and Prioritization for MTC security in Release 11**
Source: Huawei, HiSilicon, China Mobile,Interdigital,Alcatel-Lucent

Discussion:

Telecom Italia suggested focusing on the priority list and agreed with proposal 1, but disagreed with proposal 2.

The Chairman clarified that SA3 should try and work in parallel with the group.

Qualcomm and CMCC said that other aspects could be studied. He also suggested that if something is desired to be studied, it should be supported by a Study Item.

Nokia Siemens Networks reminded that SA3 is working with the outcome of SA2 so work in parallel is difficult.

It was agreed that the prioritization is clear and that further work outside should be supported by a WI.

Decision: The document was **noted**.

S3-110327 **LS on MTC USIM requirements for Release 10**
Source: C1-111155

Decision: The document was **replied to in S3-110556**.

S3-110335 **LS on MTC USIM requirements for Release 10**
Source: S1-110422

Decision: The document was **replied to in S3-110556**.

S3-110493 **Restrict the use of a USIM to specific MEs/MTC Devices**
Source: Ericsson, ST-Ericsson

Discussion:

Intel considered unsuitable relying on the IMEI for this solution as the IMEI is not tamper-proof or unclonable. Ericsson recognized this risk. CMCC asked how the IMEI can be trasfered securely and have the certainty that it cannot be cloned.

Gemalto considered premature to focus on network based solutions.

Qualcomm suggested this functionality could be used by operators if desired but is inappropriate.

There was not enough support for the R10 solution.

It was agreed to produce an LS for a reply LS (both SA1 and CT1, and CT6, plus additional interested groups).

Decision: The document was **noted**.

S3-110556 **Reply to: LS on MTC USIM requirements for Release 10**
Source: Ericsson

Decision: The document was **approved**.

S3-110332 **LS on maximum value of extended wait timer**
Source: C1-111500

Decision: The document was **noted**.

S3-110336 **LS on Release 10 NIMTC Work**
Source: GP-110382

Decision: The document was **noted**.

S3-110436 **pCR about general security requirements**
Source: ZTE Corporation

Discussion:

It was agreed to enter a reference to the SA1 requirement.

A new title was agreed to discuss issues related to restriction of use of USIM to specific MEs/MTC Devices.

Samsung volunteered to clean up the TR for the next meeting and align it to the revised SA-wide WI.

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

S3-110557 **New version of MTC Security Aspects TR**
Source: Samsung

Decision: The document was **agreed**.

S3-110437 **pCR about secure connection**
Source: ZTE Corporation, China Unicom

Discussion:

Nokia observed that GBA has already been selected and asked why GBA Push is needed. ZTE clarified this key could be used under certain situations.

Ericsson and Vodafone supported the use of GBA Push under certain scenarios.

Decision: The document was **approved**.

S3-110479 **Relation between 3GPP MTC security work and ETSI M2M**
Source: Vodafone

Discussion:

BT supported the LS drafting but pointed out that the core network in M2M is re-used but not necessarily using a UICC.

Qualcomm clarified that AT commands would not be appropriate and API would be a better way to address issues.

It was agreed to send an LS to ETSI M2M, taking into account this view from Qualcomm.

Decision: The document was **noted**.

S3-110362 **Clarification for MTC device triggering**
Source: Huawei, HiSilicon

Discussion:

Telecom Italia suggested that it should be clear that the solution does not apply to GSM as integrity protection is not provided there. InterDigital supported Telecom Italia.

It was agreed to insert an Editor's Note clarifying that the solution is intended for LTE and applicability to other technologies is FFS.

Ericsson raised concerns about the battery consumption. InterDigital proposed an Editor's Note on this issue, which was agreed.

Nokia Siemens Networks proposed adding that the MTC device reacts only to genuine messages. This was agreed.

Decision: The document was **revised to S3-110559**.

S3-110559 **Clarification for MTC device triggering**
Source: Huawei, HiSilicon

(Replaces S3-110362)

Discussion:

The last two changes agreed in the discussion in 362 have to be reflected correctly, these will go directly to the TR.

Also on the last Editor's Note, it was agreed to modify the sentence to state that the solution is intended for LTE.

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

S3-110377 **pCR to Solution 1 Triggering**
Source: China Mobile,ZTE, Interdigital

Discussion:

There were modifications on the use of TMSI for solution 1 on the second and last sentences.

There was a modification based on comments on solution 2.

A revision was agreed to be produced.

Decision: The document was **revised to S3-110560**.

S3-110560 **pCR to Solution 1 Triggering**
Source: China Mobile,ZTE, Interdigital

(Replaces S3-110377)

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

S3-110441 **pCR to MTC device Triggering Correction**
Source: China Unicom

Decision: The document was **approved**.

S3-110376 **Security requirement about small data transmission**
Source: China Mobile,ZTE,InterDigital

Discussion:

Telecom Italia suggested that progress from SA2 is awaited before deciding.

Decision: The document was **noted**.

S3-110360 **Solution for small data transmission**
Source: Huawei, HiSilicon

Discussion:

It was suggested that as for the previous contribution, progress from SA2 is awaited before deciding.

Decision: The document was **noted**.

S3-110375 **Lower power consumption security Requirement**
Source: China Mobile, ZTE,InterDigital

Discussion:

An Editor's Note was agreed to be introduced.

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

S3-110438 **Location management in MTC Monitor**
Source: ZTE Corporation

Discussion:

Further justification is necessary.

Decision: The document was **noted**.

S3-110488 **Verification of the source of the device triggering message**
Source: China Unicom, Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110440 **security issue MTC device triggering requested by MTC server**
Source: ZTE Corporation

Discussion:

Ericsson proposed taking into consideration the requirement in CR 0058 of SP-110167 as it is relevant, replacing the requirement in 440. Qualcomm and ALU supported this. There were no objections, this was agreed.

CMCC proposed an email discussion on the threat.

Decision: The document was **noted**.

S3-110361 **MTC trigger interface**
Source: Huawei, HiSilicon

Discussion:

The requirement needs to be revisited as the level of security is not clear enough. MTC device triggering was removed.

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

S3-110449 **the confidentiality protection of the external interface**
Source: CATT

Abstract:

This contribution proposals the confidentiality protection of the external interface is needed.

Decision: The document was **noted (covered by 517)**.

S3-110496 **Confidentiality protection for MTC external interface**
Source: Ericsson, ST-Ericsson

Decision: The document was **revised to S3-110517**.

S3-110517 **Confidentiality protection for MTC external interface**
Source: Ericsson, ST-Ericsson

(Replaces S3-110496)

Decision: The document was **approved**.

S3-110490 **Analysis of requirements in SA2 TR 23.888 related to external interface security**
Source: Ericsson, ST-Ericsson

Discussion:

The proposal was endorsed and will be added to the TR.

Decision: The document was **noted**.

S3-110487 **OMA DM profile for MTC devices Configuration**
Source: China Mobile, Nokia Corporation, Nokia Siemens Networks

Discussion:

An Editor's Note was agreed.

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

S3-110491 **Potential security impact with Extended paging cycles**
Source: Ericsson, ST-Ericsson

Decision: The document was **noted**.

S3-110435 **pCR to MTC Group Identifier**
Source: ZTE Corporation

Decision: The document was **withdrawn**.

S3-110439 **Security Issue - Broadcast message to a MTC group**
Source: ZTE Corporation

Decision: The document was **noted**.

S3-110558 **LS to on potential co-operation between 3GPP work on MTC security and ETSI M2M**
Source: Vodafone

Discussion:

Telecom Italia objected to attaching the WI; also Telecom Italia objected on the first bullet. On the second bullet, Telecom Italia asked to remove the word review.

BT objected on the term PLMN as it limits scenarios and possible feedback from ETSI M2M but agreed to sending the LS for the sake of progress.

Nokia Siemens Networks agreed with BT's suggestion; Vodafone suggested that this is addressed in the third bullet; Nokia Siemens Networks agreed.

Decision: The document was **approved**.

S3-110561 **LS to SA2 on confidentiality protection for MTC external device**
Source: Ericsson

Decision: The document was **approved**.

S3-110562 **LS on potential security impact with Extended paging cycles**
Source: Ericsson

Discussion:

Timeline

- 21 April: first version sent to SA3 exploder;

- 6 May: commenting deadline;

- 9 May: version with comments incorporated sent to SA3 exploder;

- 13 May: LS dispatched.

Decision: The document was **sent for email approval**.

7.10 Security Aspects of Public Warning System

The responsibility of the Rapporteurs, as requested by SA was discussed. Huawei proposed splitting the responsibility of each of the Features (tbd) among the Rapporteurs. Vodafone asked for some clarification on this split. Nokia Siemens Networks asked why two Rapporteurs are needed and proposed selecting one Rapporteur.

It was decided to have only one Rapporteur; the selection using a pseudo-randomic method; John Mattson of Ericsson will be the Rapporteur.

S3-110331 **LS on PWS security**
Source: C1-111150

Decision: The document was **noted**.

S3-110337 **Reply LS on Cell Broadcast Service for MOCN Shared Network**
Source: S2-111272

Discussion:

Vodafone noted that Shared Networks will have an impact to key management and encouraged the group to take note of the LS.

It was agreed to keep this LS in mind for PWS security.

Decision: The document was **noted**.

S3-110366 **The skeleton of PWS living document**
Source: Huawei, HiSilicon, Ericsson, ST-Ericsson

Discussion:

Nokia Siemens Networks pointed out that Features usually come before the Architecture and suggested renaming the security architecture to system architecture; Ericsson proposed renaming to system and security architecture. This was agreed.

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

S3-110363 **Security requirements of PWS**
Source: Huawei, HiSilicon

Discussion:

Vodafone asked separating the interfaces for the different messages and entities; also the requirement for authentication should be relaxed.

Telecom Italia pointed out an inconsistency between the need to authenticate and the authentication being out of scope; moreover, the latter is not a requirement.

Vodafone suggested that the requirements in SA1 should be clearly visible on the document; this was agreed. An Editor's Note was agreed on these issues raised.

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

S3-110364 **PWS security architecture overview**
Source: Huawei, HiSilicon

Discussion:

Vodafone asked changing the title of the figure; Vodafone, Qualcomm and Nokia Siemens Networks asked also for an Editor's Note to be added to state that the security architecture will describe the endpoints.

Nokia asked adding a sentence that the solution shall have no impact on security features on existing base stations.

There was no agreement on the above: the three bullets on system architecture were removed and the picture and title were kept. TeliaSonera asked whether this picture will be updated according to the decisions; it was agreed to amend the Editor's Note to state that the figure might be modified.

The rest of the contribution was approved.

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

S3-110365 **Security features of PWS**
Source: Huawei, HiSilicon

Discussion:

Nokia asked removing the UE related sentences and amending the heading. It was agreed to insert an Editor's Note that algorithm negotiation has to be avoided.

NTT Docomo asked toi insert a second Editor's Note,; this was agreed.

Decision: The document was **revised to S3-110566**.

S3-110566 **Security features of PWS**
Source: Huawei, HiSilicon

(Replaces S3-110365)

Decision: The document was **approved**.

S3-110394 **Distribution of keys for protecting public warning messages**
Source: Vodafone

Discussion:

Nokia Siemens Networks liked the proposed mechanism, but asked what would be the attacking scenario directed at; Vodafone replied that the attack scenario has in mind public events, where a sufficient of number of users to create confusion or panic is present.

Vodafone reminded that the threat of false base stations is still a valid threat, but the work effort required is higher.

Ericsson asked why sending the key in clear and then protecting the messages. Vodafone replied that the intention is to investigate potential solutions.

NTT Docomo asked how often should the refreshing of the key be done; Vodafone replied that this event would happen rarely.

Huawei supported studying the subject further; there were no objections; this was agreed.

Vodafone suggested adding robustness requirements from clause 2; this was agreed; Nokia asked to insert some text to address overloads; this was agreed.

TeliaSonera proposed adding the requirement for test warning messages; this was agreed.

Decision: The document was **noted**.

S3-110462 **PWS Digital Signature Profile**
Source: Ericsson, ST-Ericsson

Discussion:

Vodafone pointed out that the length limit is valid only for ETWS, not PWS; Huawei expressed concerns about the length proposed and proposed the use of other algorithms than DSA.

Nokia proposed considering ECC; Ericsson pointed out that in the paper it is stated that ECDSA does not provide shorter signatures. NTT Docomo asked whether this is valid for ECDSA or for ECC as a whole and proposed consulting ETSI SAGE. Vodafone asked waiting for the next meeting to have a clearer list of requirements before contacting ETSI SAGE. Ericsson agreed to this.

The paper was noted, but it was agreed to insert in the living document the potential limits in the paper.

Decision: The document was **noted**.

S3-110565 **New version of PWS security living document**
Source: Huawei

Discussion:

Nokia asked for an Editor's Note in 5.1.2.3 to state that the feasibility of signature verification in the UE is FFS.

Decision: The document was **approved**.

7.11 Other Areas

S3-110317 **Response LS on Security and Authentication in UDC**
Source: C4-102710

Discussion:

It was proposed to note 317 and 319 and act only should there be further requests on the topic. This was agreed.

Decision: The document was **noted**.

S3-110319 **Encryption algorithms for UDC**
Source: SAGE-10-09

Decision: The document was **noted**.

S3-110318 **Reply LS on review of MDT design and reply LS on Security Issues with Logged MDT**
Source: S5-110529

Decision: The document was **noted**.

S3-110320 **Reply LS on MDT user involvement (S5-110367 / R2-110699)**
Source: S5-110482

Decision: The document was **noted**.

S3-110328 **Reply LS for MDT**
Source: S1-110172

Decision: The document was **noted**.

S3-110346 **LS on MDT User consent handling**
Source: S5-111525

Decision: The document was **noted**.

S3-110340 **LS on User consent indication for MDT**
Source: R3-110931

Decision: The document was **noted**.

S3-110463 **LS on MDT configuration with user consent**
Source: R2-111714

Decision: The document was **noted**.

S3-110464 **Reply to: Reply LS on Interaction with Trace for MDT (S5-111097 / S3-110203)**
Source: S5-111522

Decision: The document was **noted**.

S3-110344 **Liaison statement on user consent in area or management based MDT activation**
Source: SP-110230

Decision: The document was **replied to in S3-110564**.

S3-110350 **Privacy Considerations in Management / Area MDT**
Source: Nokia Corporation, Nokia Siemens Networks

Abstract:

Discussion paper to provide some background for a potential LS answer on MDT

Decision: The document was **noted**.

S3-110524 **Comments on S3-110350 Privacy Considerations in Management / Area MDT**
Source: NEC Corporation

Decision: The document was **noted**.

S3-110456 **Discussion of MDT incoming LSs**
Source: NTT docomo

Abstract:

This contribution gives a summary of the actions on SA3 in incoming LSs on MDT. It reconfirms the guidance given in S3-110185.

Decision: The document was **noted**.

S3-110512 **Comments to Discussion of MDT privacy requirements (S3-110456)**
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

NTT Docomo pointed out the user consent on the eNB is necessary, even in the case of area based MDT. Deutsche Telekom would prefer to have user consent. Nokia suggested that as the data is anonymised regulations would not require user consent. It was suggested that this kind of information does not fall under the category of value added service and would not require user consent.

Orange suggested that management MDT is identifying a user and on even uncorrelated, on the network side it can be possible to retrieve the identity of the user. Vodafone pointed out that the data is collected before it can be anonymized, which could create legal implications. Nokia suggested that user consent and anonymization could be combined. NEC preferred the user consent approach. NTT Docomo suggested that if the mechanisms could not be used in areas with few users it would be a drawback.

It was agreed that there will be no collection for roaming users.

Decision: The document was **noted**.

S3-110457 **draft Reply LS on MDT privacy**
Source: NTT docomo

Abstract:

This draft reply LS deals with all actions in the incoming LSs on MDT security and reconfirm SA3 guidance given in S3-110185

Decision: The document was **revised to S3-110564**.

S3-110564 **Reply to: Liaison statement on user consent in area or management based MDT activation**
Source: NTT Docomo

Decision: The document was **revised to S3-110575**.

S3-110575 **Reply to: Liaison statement on user consent in area or management based MDT activation**
Source: NTT Docomo

(Replaces S3-110564)

Decision: The document was **approved**.

S3-110325 **Reply LS on LCLS optional functionality in BSS**
Source: SA3LI11_059r1

Decision: The document was **noted**.

S3-110338 **Reply LS on Liaison Statement on security issues of PSS service**
Source: S4-110335

Decision: The document was **noted**.

S3-110339 **Reply LS on Requirements and Architecture issues of PSS service**
Source: S1-110175

Discussion:

A reply LS was considered; a decision will be taken later during the meeting.

Decision: The document was **replied to in S3-110572**.

S3-110572 **Reply LS on Requirements and Architecture issues of PSS service**
Source: Ericsson

Decision: The document was **approved**.

S3-110495 **33.110: Description in normative annex A of the key to be used in KDF**
33.110 CR-0018 (Rel-9) v9.0.0
Source: Gemalto, Verizon

Abstract:

CR to 33.110: Description in normative annex A of the key to be used in KDF

Decision: The document was **revised to S3-110569**.

S3-110569 **33.110: Description in normative annex A of the key to be used in KDF**
33.110 CR-0018 rev 1 (Rel-9) v9.0.0
Source: Gemalto, Verizon

(Replaces S3-110495)

Decision: The document was **agreed**.

S3-110570 **33.110: Description in normative annex A of the key to be used in KDF**
33.110 CR-0019 (Rel-11) v10.0.0
Source: Gemalto, Verizon

Decision: The document was **agreed**.

8 Studies

8.1 UTRAN Key Management Enhancements

S3-110425 **UKM Solution 1 Cleanup**
Source: ZTE Corporation

Decision: The document was **approved**.

S3-110429 **SRNS relocation without UE involvement for simplified forward security based solution**
Source: ZTE Corporation

Decision: The document was **approved**.

S3-110426 **IWK with GERAN E-UTRAN for simplified forward security based solution**
Source: ZTE Corporation

Discussion:

Some editorial modifications proposed by Ericsson were agreed.

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

S3-110427 **Updates of changes to messages of the simplified forward security base solution**
Source: ZTE Corporation

Discussion:

Qualcomm pointed out that applying changes to SMC would impact stage 3, whereas other solutions would avoid this. It was agreed to insert an Editor's Note on that issue.

It was also agreed not to include the changes in 5.4.5.2.

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

S3-110371 **Add the support of the enhanced UTRAN security context of ME to SMC message (S3-110081)**
Source: Huawei,HiSilicon, ZTE corporation

Discussion:

A note was agreed on the fact that SMC modification would have RAN impact.

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

S3-110372 **pCR to 5.2.3.1.2 - the time to perform AKA(S3-110082)**
Source: Huawei,HiSilicon,ZTE corporation

Decision: The document was **approved**.

S3-110466 **Editorial corrections and clarifications to TR 33.859**
Source: Ericsson, ST-Ericsson

Decision: The document was **approved**.

S3-110428 **Comparison table of changes to messages for 3 solutions**
Source: ZTE Corporation

Discussion:

An Editor's Note added to the comparison table on the fact that further work is needed.

The conclusions were removed.

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

S3-110423 **Comparison of proposed solutions signals and compatibility aspects**
Source: ZTE Corporation

Decision: The document was **approved**.

S3-110424 **Security threats analysis**
Source: ZTE Corporation

Decision: The document was **approved**.

S3-110408 **pCR on impact on EPS**
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

Qualcomm proposed splitting the effect on LTE; Ericsson supported this.

The first and third Editor's Note's were agreed.

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

S3-110489 **Clarifying enhancements to the MME in UTRAN KH study**
Source: Qualcomm Incorporated

Decision: The document was **approved**.

S3-110500 **Updating the system overview for TR 33.859**
Source: Ericsson, ST-Ericsson

Discussion:

The requirement in 4.2 was removed.

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

S3-110401 **Methodology for the evaluation of UTRAN security enhancements**
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

It was agreed that platform security will be an assumption for this work.

Decision: The document was **noted**.

S3-110522 **COMMENTS on Methodology for the evaluation of UTRAN security enhancements**
Source: Ericsson, ST-Ericsson, ZTE Corporation

Decision: The document was **noted**.

S3-110402 **pCR on introducing platform security**
Source: Nokia Corporation, Nokia Siemens Networks

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

S3-110403 **pCR on evaluation of proposed measure wrt use case of stationary users**
Source: Nokia Corporation, Nokia Siemens Networks

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

S3-110404 **pCR on evaluation of proposed measure wrt use case of moving user**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110405 **pCR on evaluation wrt target orientation**
Source: Nokia Corporation, Nokia Siemens Networks

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

S3-110406 **pCR on evaluation wrt penetration**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110407 **pCR on Comparing solution 2 to increasing the authentication frequency**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110492 **Analysis of CN and RN level key separation in UTRAN KH**
Source: Qualcomm Incorporated

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

S3-110571 **New version of UKH TR**
Source: Ericsson (Rapporteur)

Discussion:

Timeline:

- 20 April - version sent on SA3 exploder;

- 6 May - commenting deadline;

- 13 May - final implementation.

Decision: The document was **sent for email approval**.

8.2 Extended Identity Management

S3-110349 **Correction of Ua security protocol identifier for OpenID-GBA Interworking**
33.924 CR-16 (Rel-9) v9.3.0
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

NTT Docomo pointed out the protocol identifier should be checked; Nokia will check and revise the CR if necessary; the content of the CR is agreed.

In addition, an R10 mirror would be necessary.

Decision: The document was **merged in S3-110576**.

S3-110485 **33.924 CR (R10): Alignment of HTTPS usage in GBA OpenID interworking**
33.924 CR-17 (Rel-10) v9.3.0
Source: Ericsson, ST-Ericsson

Discussion:

Deutsche Telekom pointed out this CR impacts CR0016; this has to be checked.

After some offline discussions it was decided to merge 485 and 349.

Decision: The document was **revised to S3-110576**.

S3-110576 **33.924 CR (R9): Correction of UA security protocol identifier in GBA - OpenID interworking**
33.924 CR-19 (Rel-9) v9.3.0
Source: Ericsson, ST-Ericsson

(Replaces S3-110485)

Decision: The document was **agreed**.

S3-110577 **33.924 CR (R10): Correction of UA security protocol identifier in GBA - OpenID interworking**
33.924 CR-20 (Rel-10) v10.0.0
Source: Ericsson, ST-Ericsson

(Replaces S3-110485)

Decision: The document was **agreed**.

S3-110486 **33.924 CR (R10): Relationship of identities in GBA OpenID interworking**
33.924 CR-18 (Rel-10) v9.3.0
Source: Ericsson, ST-Ericsson

Discussion:

It was agreed for the first option to be limited to the operator network, and for the second option to clarify the text.

Decision: The document was **revised to S3-110574**.

S3-110574 **33.924 CR (R10): Relationship of identities in GBA OpenID interworking**
33.924 CR-18 rev 1 (Rel-10) v10.0.0
Source: Ericsson, ST-Ericsson

(Replaces S3-110486)

Decision: The document was **agreed**.

8.3 Extended IMS media plane security features

It was decided to send the documents that were not handled during the meeting, belonging to this study item, for email approval.

The process for this email approval will be as follows:

- the documents appearing on the list here below are sent for email approval;

(S3-110430 is not on the list as it is a discussion paper and can be consulted in conjunction with S3-110431, but is considered as noted);

- the deadline for comments is 11 May;

- comments have to be sent to the exploder with a clear indication on the subject line mentioning the S3-11xxxx number to which the comment applies;

- sources can send revised versions of the pCR, according to comments; revised versions should have rN after the S3 number (e.g. S3-110430r1, S3-110430r2, ...);

- After the deadline of 11 May and by the 16th of May, each source will announce the result of the email approval of each of their documents (these can be: approved, noted, approved with modifications).

  * If the contribution is approved with modifications, the modifications have to be listed;

  * If the contribution is approved with modifications and there has been a revised pCR made available on the exploder, the S3-110xxxrN version should be mentioned;

  * If there is still no consensus on the contribution on May 11, the contribution will have to be announced as noted by the source;

  * If there have been no comments on the contribution, the contribution will have to be announced as approved by the source.

- all approved (and approved with modifications) contributions will be implemented by the Rapporteur in S3-110578, which will then follow the rest of the timeline reported here below.

The timeline for this approval will be as follows:

- 20 April email approval initiation;

- 11 May - commenting deadline;

- 16 May - sources provide revised pCRs (for pCRs that have had comments);

- 20 May - TR Rapporteur provides new version according to approved documents;

- 27 May - commenting deadline on TR;

- 6 June - TR final version is provided.

S3-110324 **LS on LI requirements related to encryption**
Source: SA3LI11_058r1

Decision: The document was **replied to in S3-110573**.

S3-110308 **Draft reply LS on LI requirements related to encryption**
Source: Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell

Abstract:

This contribution analyses the recommendation by SA WG3-LI on applicability of MitM for LI purposes.

Decision: The document was **revised to S3-110573**.

S3-110573 **Reply to: LS on LI requirements related to encryption**
Source: BT

Decision: The document was **approved**.

S3-110411 **Pseudo CR for TR 33.829: Security Policies for Conferencing**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **sent for email approval**.

S3-110412 **Pseudo CR for TR 33.829: Enhanced Description of the SDES Based Solution for Conferencing**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **sent for email approval**.

S3-110470 **TR 33.829: KMS conference group key update**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110471 **TR 33.829: KMS conference group keying support**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110472 **TR 33.829: Protection of event packages**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110473 **TR 33.829: Conference system interfaces**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110474 **TR 33.829: KMS Mutual authentication with MIKEY-TICKET (RFC 6043)**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110475 **TR 33.829: KMS Update of allowed conference participants**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110476 **TR 33.829: KMS Clarification conference call out**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110477 **TR 33.829: KMS conference signalling**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110430 **pCR on TR33.829- discussion paper of secure SRVCC**
Source: ZTE Corporation

Decision: The document was **noted**.

S3-110431 **pCR on TR33.829 - e2e security solution for SRVCC**
Source: ZTE Corporation

Decision: The document was **sent for email approval**.

S3-110310 **Clarification of requirements and capabilities for clause 7.1**
Source: Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell

Abstract:

There is an Editors note in clause 7.1 stating that: More details are needed on the requirements and how the currently standardized solutions can address them. It is proposed that the changes in the PCR are approved and included in the TR.

Decision: The document was **sent for email approval**.

S3-110309 **pCR to TR 33.mps Services for user groups with high security requirements**
Source: Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell

Abstract:

This document provides a potential solution for services for user groups with high security requirements described in Section 7 of TR 33.mps.

Decision: The document was **sent for email approval**.

S3-110413 **Pseudo CR for TR 33.829: Minor Changes to the Messaging Description**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **sent for email approval**.

S3-110414 **Pseudo CR for TR 33.829: Solution Proposal for Messaging**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **sent for email approval**.

S3-110460 **KMS Based Immediate Messaging Protection**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110461 **KMS Based Session-Based Messaging Protection**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110458 **IANA MIKEY Assignments**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110459 **Pre-Shared Key MIME Protection**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110409 **Pseudo CR to TR 33.829: Impact of Communications Diversion (CDIV) on peer identification**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **sent for email approval**.

S3-110410 **Pseudo CR to TR 33.829: More detailed discussion of the SDES solution for CDIV**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **sent for email approval**.

S3-110478 **TR 33.829: KMS call diversion solution 2 update**
Source: Ericsson, ST-Ericsson

Decision: The document was **sent for email approval**.

S3-110578 **New version of TR on IMS Media Security**
Source: Vodafone

Decision: The document was **sent for email approval**.

8.4 SSO Applications Security for IMS – based on SIP Digest

S3-110373 **P-CR Improvements for Solution1**
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

Telecom Italia asked for some clarification on Note 3.

IDC asked adding an Editor's Note on the fact that the solution provides MiTM after the use of the Ks; Ericsson supported this. Nokia Siemens Networks suggested this is addressed in 4.1.6. Ericsson replied they are aware of this text but preferred for an Editor's Note.

The Editor's Note would read: channel binding of the authentication response RESP needs FFS; this Editor's Note was agreed.

CMCC requested removing step 0; Nokia Siemens Networks replied that removing the TLS tunnel would completely change the solution. It was agreed to insert this solution and leave open the possibility for other solutions to be considered at the next meeting.

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

S3-110416 **Derivation of authentication response and key Ks in Non-UICC based GBA solution**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110444 **pCR to TR33.914 - solution update of Section 7.2.1**
Source: China Mobile

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

S3-110447 **Improvement to solution 1 using protocol binding of SIP digest over TLS n TR 33.914**
Source: InterDigital

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

S3-110494 **Structure clarifications to SIP digest based GBA**
Source: Ericsson, ST-Ericsson

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

S3-110443 **pCR to TR33.914 - interface consideration of Section 7.2.1**
Source: China Mobile,Nokia Corporation,Nokia Siemens Networks

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

S3-110445 **pCR to TR33.914 - advantages of non-UICC base GBA in Section 7.2.2**
Source: China Mobile,Nokia Corporation,Nokia Siemens Networks

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

S3-110432 **Optimization of implementing SSO_APS based on SIP Digest**
Source: ZTE Corporationï¼ŒChina Unicom

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

S3-110433 **Architecture for interworking with OpenID**
Source: ZTE Corporation, China Unicom

Discussion:

Nokia and InterDigital suggested the architecture proposed seemed interesting, but could not understand what was the exact proposal and which part of the document it would be addressing.

Decision: The document was **noted**.

S3-110434 **Interworking message flow with OpenID**
Source: ZTE Corporation, China Unicom

Discussion:

Nokia proposed this should not belong to the evaluation clause. ZTE proposed clause 7.3.4 Vodafone suggested this is related to 433.

433 and 434 should be merged and address solution 3; this should be done for the next meeting.

Decision: The document was **noted**.

S3-110448 **Improvement to SIP digest SSO solution in section 7.3.2 with RP authentication details**
Source: InterDigital

Discussion:

An Editor's Note was approved.

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

S3-110583 **Merger of 373, 443, 444, 445, 494**
Source: Nokia

Discussion:

This contribution was created to provide guidance on how the pCRs would results in the new version of the TR and was noted.

Decision: The document was **noted**.

S3-110581 **New version of TR on Study on Single Sign On (SSO) Application Security for IMS - based on SIP Digest**
Source: Nokia

Discussion:

It was agreed to send the email approved version for email approval.

Timeline for the email approval:

- 20 April - version sent on SA3 exploder;

- 6 May - commenting deadline;

- 13 May - final implementation.

Decision: The document was **sent for email approval**.

8.5 Study on Security aspects of Integration of Single Sign-On (SSO) frameworks with 3GPP networks

S3-110322 **Response liaison statement to 3GPP TSG SA on OpenID interworking with AKA**
Source: COM13-LS147

Discussion:

It was decided that further discussion is needed in the next meeting and a reply was not approved at the present meeting.

Decision: The document was **postponed to the next meeting**.

S3-110552 **Void**
Source: Void

Decision: The document was **withdrawn**.

S3-110532 **Reply LS to COM13-LS147 Response liaison statement on OpenID interworking with AKA**
Source: Alcatel-Lucent

Decision: The document was **withdrawn**.

S3-110323 **Answer to Liaison Statement regarding 3GPP SSO integration without GBA**
Source: OMA-LS_896-OMA_ARC_to_3GPP_SA3_OpenID-20110209-A

Discussion:

Nokia will inform the leadership of OMA ARC SEC SWG of the proceedings in SA3.

Decision: The document was **postponed to the next meeting**.

S3-110505 **Types of credentials for the SSO study**
Source: Ericsson, ST-Ericsson

Discussion:

It was decided to have an email approval to send an LS to SA1.

Decision: The document was **noted**.

S3-110579 **LS on clarification of type(s) of operator-controlled SSO credentials**
Source: Ericsson

Discussion:

Timeline:

20 April - first version provided;

4 May - commenting deadline;

6 May - final version provided.

Decision: The document was **sent for email approval**.

S3-110507 **Relation of SSO TR to other work in 3GPP**
Source: Ericsson, ST-Ericsson

Decision: The document was **approved**.

S3-110347 **P-CR Generic Terminal Requirements for using UICC credentials for SSO from a browser**
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

Consensus could not be reached in this meeting. Offline discussion on the way forward is encouraged.

Decision: The document was **noted**.

S3-110509 **Comments on S3-110347, 'P-CR Generic Terminal Requirements for using UICC credentials for SSO from a browser'**
Source: Alcatel-Lucent, AT&T

Decision: The document was **noted**.

S3-110348 **P-CR Collocated GBA Architecture**
Source: Nokia Corporation, Nokia Siemens Networks

Discussion:

Consensus could not be reached and further discussion is encouraged to reach agreement in the next meeting.

Decision: The document was **noted**.

S3-110501 **GBA Lite**
Source: Ericsson, ST-Ericsson, AT&T, Roger Wireless

Discussion:

Consensus could not be reached and further discussion is encouraged to reach agreement in the next meeting.

Decision: The document was **noted**.

S3-110511 **Comments to GBA Lite (S3-110501)**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110306 **pCR to TR 33.sso Section 8, Solutions**
Source: Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell, Rogers Wireless

Abstract:

This contribution fills in Clause 8, Solutions for OpenID 3GPP interworking, in the Study on Security aspects of integration of Single Sign-On (SSO) frameworks with 3GPP operator-controlled resources and mechanisms.

Discussion:

It was decided to note the contribution. It was also decided to hold an email discussion on item 8.5. AT&T will chair this email discussion.

Decision: The document was **noted**.

S3-110513 **Comments to pCR to TR 33.sso Section 8, Solutions (S3-110306)**
Source: Nokia Corporation, Nokia Siemens Networks

Decision: The document was **noted**.

S3-110580 **New version of TR on Study on Security aspects of Integration of Single Sign-On (SSO) frameworks with 3GPP networks**
Source: Ericsson

Discussion:

Timeline:

- 20 April - version sent on SA3 exploder;

- 6 May - commenting deadline;

- 13 May - final implementation.

Decision: The document was **sent for email approval**.

8.6 Security Aspects in the Scope of the SA2 study on IMS Based Peer-to-Peer Content (SP-100567)

8.7 Other Study Areas

9 Review and Update of Work Plan

S3-110303 **SA3 WorkPlan**
Source: WG Secretary

Discussion:

Rapporteurs are invited to provide input on progress of the work items.

Decision: The document was **noted**.

S3-110510 **Guidelines for SA3 Delegates v020**
Source: MCC

Decision: The document was **noted**.

10 Future Meeting Dates and Venues

S3-110304 **SA3 Meeting Calendar**
Source: SA3 Secretary

Decision: The document was **revised to S3-110582**.

S3-110582 **SA3 Meeting Calendar**
Source: SA3 Secretary, SA3 Chairman

(Replaces S3-110304)

Discussion:

As per some discussions with CT and SA2 leadership it was decided to attempt and co-locate as much as possible, especially when close to stage 2 freezing deadlines. It was noted that this creates a problem for MCC as support of multiple WGs becomes difficult.

T

Decision: The document was **approved**.

11 Any Other Business

There was no other business.

12 Close

The Chairman thanked the host, China Mobile and CATT, for hosting the meeting in the lovely city of Chengdu, China. He also thanked the Secretary and the Delegates for their hard work and contributions during the meeting.

The meeting was closed.

Annex A: List of contribution documents

Document	Title	Source	Decision	Replaces	Replaced by
S3-110300	Draft Agenda for THIS meeting	WG Chairman	approved	-	-
S3-110301	Report from LAST SA Plenary	WG Chairman	noted	-	-
S3-110302	Report from LAST SA3 Ordinary meeting	WG Secretary	approved	-	-
S3-110303	SA3 WorkPlan	WG Secretary	noted	-	-
S3-110304	SA3 Meeting Calendar	SA3 Secretary	revised	-	S3-110582
S3-110305	H(e)NB. Security of direct interfaces	Alcatel-Lucent, Alcatel-Lucent Shanghai Bell	noted	-	-
S3-110306	pCR to TR 33.sso Section 8, Solutions	Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell, Rogers Wireless	noted	-	-
S3-110307	A way forward for the treatment of the newly discovered vulnerability due to undefined H(e)NB Identity binding to H(e)NB-GW	Alcatel-Lucent, AT&T, Vodafone, Alcatel-Lucent Shanghai Bell	noted	-	-
S3-110308	Draft reply LS on LI requirements related to encryption	Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell	revised	-	S3-110573
S3-110309	pCR to TR 33.mps Services for user groups with high security requirements	Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell	sent for email approval	-	-
S3-110310	Clarification of requirements and capabilities for clause 7.1	Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell	sent for email approval	-	-
S3-110311	Corrective text for undefined wording - autonomous validation of RN platform	InterDigital, China Mobile, Nokia Siemens Networks	revised	-	S3-110534
S3-110312	Removal of Hosting Party Authentication, R9	Qualcomm Incorporated	noted	-	-
S3-110313	Removal of Hosting Party Authentication, R10	Qualcomm Incorporated	noted	-	-
S3-110314	Location Verification Correction, R9	Qualcomm Incorporated	withdrawn	-	-
S3-110315	Location Verification Correction, R10	Qualcomm Incorporated	withdrawn	-	-
S3-110316	Location Verification Correction, R11	Qualcomm Incorporated	withdrawn	-	-
S3-110317	Response LS on Security and Authentication in UDC	C4-102710	noted	-	-
S3-110318	Reply LS on review of MDT design and reply LS on Security Issues with Logged MDT	S5-110529	noted	-	-
S3-110319	Encryption algorithms for UDC	SAGE-10-09	noted	-	-
S3-110320	Reply LS on MDT user involvement (S5-110367 / R2-110699)	S5-110482	noted	-	-
S3-110321	LS reply on OAM architecture aspects for RNs (S5-110067 / R3-102541)	S5-110546	noted	-	-
S3-110322	Response liaison statement to 3GPP TSG SA on OpenID interworking with AKA	COM13-LS147	postponed to the next meeting	-	-
S3-110323	Answer to Liaison Statement regarding 3GPP SSO integration without GBA	OMA-LS_896-OMA_ARC_to_3GPP_SA3_OpenID-20110209-A	postponed to the next meeting	-	-
S3-110324	LS on LI requirements related to encryption	SA3LI11_058r1	replied to	-	-
S3-110325	Reply LS on LCLS optional functionality in BSS	SA3LI11_059r1	noted	-	-

S3-110326	Reply LS on Relay Node OAM System Discovery	R3-110968	noted	-	-
S3-110327	LS on MTC USIM requirements for Release 10	C1-111155	replied to	-	-
S3-110328	Reply LS for MDT	S1-110172	noted	-	-
S3-110329	Reply LS on OAM architecture aspects for RNs	R3-110970	noted	-	-
S3-110330	Reply LS on Security for LTE relay nodes	R3-111034	noted	-	-
S3-110331	LS on PWS security	C1-111150	noted	-	-
S3-110332	LS on maximum value of extended wait timer	C1-111500	noted	-	-
S3-110333	LS on partial success of Write Replace Warning Request for ETWS	R3-111084	noted	-	-
S3-110334	Reply LS on Simultaneous registration of a single private identity from different UEs	S2-111153	noted	-	-
S3-110335	LS on MTC USIM requirements for Release 10	S1-110422	replied to	-	-
S3-110336	LS on Release 10 NIMTC Work	GP-110382	noted	-	-
S3-110337	Reply LS on Cell Broadcast Service for MOCN Shared Network	S2-111272	noted	-	-
S3-110338	Reply LS on Liaison Statement on security issues of PSS service	S4-110335	noted	-	-
S3-110339	Reply LS on Requirements and Architecture issues of PSS service	S1-110175	replied to	-	-
S3-110340	LS on User consent indication for MDT	R3-110931	noted	-	-
S3-110341	LS on excessive updates of NAS security context	C6-110184	replied to	-	-
S3-110342	LS on additional considerations of Relay Nodes in the LTE-Advanced material for Rec. ITU-R M.[IMT.RSPEC] to be submitted to ITU-R WP5D#10 (6-13 April, 2011)	RP-110006	noted	-	-
S3-110343	Reply LS on MTC Planning and Prioritization	SP-110218	noted	-	-
S3-110344	Liaison statement on user consent in area or management based MDT activation	SP-110230	replied to	-	-
S3-110345	LS on Network Sharing	SP-110234	noted	-	-
S3-110346	LS on MDT User consent handling	S5-111525	noted	-	-
S3-110347	P-CR Generic Terminal Requirements for using UICC credentials for SSO from a browser	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110348	P-CR Collocated GBA Architecture	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110349	Correction of Ua security protocol identifier for OpenID-GBA Interworking	Nokia Corporation, Nokia Siemens Networks	merged in S3-110576	-	-
S3-110350	Privacy Considerations in Management / Area MDT	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110351	DISC-Analysis on binding of UICC and RN	Huawei, HiSilicon	noted	-	-
S3-110352	CR-Detailed binding of RN and UICC	Huawei, HiSilicon	revised	-	S3-110536
S3-110353	DISC-Clarification on initial attach procedure for PSK case	Huawei, HiSilicon	noted	-	-
S3-110354	CR-Clarification on initial attach procedure for PSK case	Huawei, HiSilicon	revised	-	S3-110541
S3-110357	Algorithm negotiation on Un interface	Huawei, HiSilicon	noted	-	-
S3-110358	CR-Algorithm negotiation on Un	Huawei, HiSilicon	withdrawn	-	-

	interface				
S3-110359	Discussion on excessive update of NAS Security Context in the LS C6-110184	Huawei, HiSilicon	noted	-	-
S3-110360	Solution for small data transmission	Huawei, HiSilicon	noted	-	-
S3-110361	MTC trigger interface	Huawei, HiSilicon	approved with modifications	-	-
S3-110362	Clarification for MTC device triggering	Huawei, HiSilicon	revised	-	S3-110559
S3-110363	Security requirements of PWS	Huawei, HiSilicon	approved with modifications	-	-
S3-110364	PWS security architecture overview	Huawei, HiSilicon	approved with modifications	-	-
S3-110365	Security features of PWS	Huawei, HiSilicon	revised	-	S3-110566
S3-110366	The skeleton of PWS living document	Huawei, HiSilicon, Ericsson, ST-Ericsson	approved with modifications	-	-
S3-110367	Removal of mandatory support for HTTPS in CMP transport-R9	Huawei, HiSilicon, Nokia Corporation, Nokia Siemens Networks	revised	-	S3-110567
S3-110368	Removal of mandatory support for HTTPS in CMP transport-R10	Huawei, HiSilicon,Nokia Corporation, Nokia Siemens Networks	revised	-	S3-110568
S3-110369	CMPv2 message format	Huawei, HiSilicon	noted	-	-
S3-110370	Security of direct interface between H(e)NBs	Huawei, HiSilicon	noted	-	-
S3-110371	Add the support of the enhanced UTRAN security context of ME to SMC message (S3-110081)	Huawei,HiSilicon, ZTE corporation	approved with modifications	-	-
S3-110372	pCR to 5.2.3.1.2 - the time to perform AKA(S3-110082)	Huawei,HiSilicon,ZTE corporation	approved	-	-
S3-110373	P-CR Improvements for Solution1	Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110375	Lower power consumption security Requirement	China Mobile, ZTE,InterDigital	approved with modifications	-	-
S3-110376	Security requirement about small data transmission	China Mobile,ZTE,InterDigital	noted	-	-
S3-110377	pCR to Solution 1 Triggering	China Mobile,ZTE, Interdigital	revised	-	S3-110560
S3-110378	Clarification of certificate and subscription handling	China Mobile,Nokia Siemens Networks, Nokia Corporation	revised	-	S3-110539
S3-110379	Correction of reference for key usage bit in TLS certificate and some editorials	Nokia Corporation, Nokia Siemens Networks	agreed	-	-
S3-110380	Correction on CRL distribution point for vendor root CA certificates	Nokia Corporation, Nokia Siemens Networks	agreed	-	-
S3-110381	[33.210] Clarification of algorithm names and DH group usage in IKEv2	Nokia Corporation, Nokia Siemens Networks	agreed	-	-
S3-110382	[33.210, rel-10] Correction of Iuh/Iurh security	Nokia Corporation, Nokia Siemens Networks	agreed	-	-
S3-110383	[33.210, rel-11] Correction of Iuh/Iurh security	Nokia Corporation, Nokia Siemens Networks	agreed	-	-
S3-110384	Security mechanism for H(e)NB no-IPsec usage option	Samsung	noted	-	-
S3-110385	Security mechanism for H(e)NB no-IPsec usage option [Rel-9]	Samsung	revised	-	S3-110547
S3-110386	Security mechanism for H(e)NB no-IPsec usage option [Rel-10]	Samsung	revised	-	S3-110548
S3-110387	Security mechanism for H(e)NB no-IPsec usage option [Rel-11]	Samsung	revised	-	S3-110549
S3-110388	Disc - A5/3 and A5/4 support in	Orange	noted	-	-

	GSM				
S3-110389	CR - A5/3 and A5/4 support in GSM	Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera	revised	-	S3-110553
S3-110390	H(e)NB-LGW Remote IP Address Assignment [Rel-10]	Samsung, Qualcomm	noted	-	-
S3-110391	H(e)NB-LGW Remote IP Address Assignment [Rel-11]	Samsung, Qualcomm	noted	-	-
S3-110392	Update of SIMTC WID	Samsung	revised	-	S3-110555
S3-110393	DRAFT LS on CSG security for H(e)NB	Alcatel-Lucent, Alcatel-Lucent Shanghai Bell	revised	-	S3-110545
S3-110394	Distribution of keys for protecting public warning messages	Vodafone	noted	-	-
S3-110395	Resolution of Editor's Notes for PDPC integrity for Relay Nodes	Nokia Siemens Networks	revised	-	S3-110535
S3-110396	Corrections to communication between MME and DeNB for relay nodes	Nokia Siemens Networks, China Mobile, Gemalto	merged in 520	-	-
S3-110397	Specification of secure channel profiles and certificates used for Relay nodes (RNs) and UICC (USIM-RN)	Nokia Siemens Networks	revised	-	S3-110537
S3-110398	Resolution of Editor's Notes for Relay Node security procedures	Nokia Siemens Networks, China Mobile	revised	-	S3-110542
S3-110399	Corrections and Clarifications for Relay Node security procedures	Nokia Siemens Networks, Gemalto	revised	-	S3-110543
S3-110400	Correction on communication outside secure channel for Relay Node security procedures	China Mobile, Gemalto, InterDigital Communications, Nokia Siemens Networks, Sagem-Orga	revised	-	S3-110538
S3-110401	Methodology for the evaluation of UTRAN security enhancements	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110402	pCR on introducing platform security	Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110403	pCR on evaluation of proposed measure wrt use case of stationary users	Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110404	pCR on evaluation of proposed measure wrt use case of moving user	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110405	pCR on evaluation wrt target orientation	Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110406	pCR on evaluation wrt penetration	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110407	pCR on Comparing solution 2 to increasing the authentication frequency	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110408	pCR on impact on EPS	Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110409	Pseudo CR to TR 33.829: Impact of Communications Diversion (CDIV) on peer identification	Nokia Corporation, Nokia Siemens Networks	sent for email approval	-	-
S3-110410	Pseudo CR to TR 33.829: More detailed discussion of the SDES solution for CDIV	Nokia Corporation, Nokia Siemens Networks	sent for email approval	-	-
S3-110411	Pseudo CR for TR 33.829: Security Policies for Conferencing	Nokia Corporation, Nokia Siemens Networks	sent for email approval	-	-
S3-110412	Pseudo CR for TR 33.829: Enhanced Description of the SDES Based Solution for Conferencing	Nokia Corporation, Nokia Siemens Networks	sent for email approval	-	-

S3-110413	Pseudo CR for TR 33.829: Minor Changes to the Messaging Description	Nokia Corporation, Nokia Siemens Networks	sent for email approval	-	-
S3-110414	Pseudo CR for TR 33.829: Solution Proposal for Messaging	Nokia Corporation, Nokia Siemens Networks	sent for email approval	-	-
S3-110415	SPUCI: Technical and Non-Technical Prevention Measures	Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110416	Derivation of authentication response and key Ks in Non-UICC based GBA solution	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110417	Analysis of MTC Planning and Prioritization for MTC security in Release 11	Huawei, HiSilicon, China Mobile,Interdigital,Alcatel-Lucent	noted	-	-
S3-110418	CR-Security handling for relay related UE handover	Huawei, HiSilicon	noted	-	-
S3-110419	Security handling for UE handover from Relay	Huawei, HiSilicon	noted	-	-
S3-110420	Correction of the RN attach procedure	ZTE Corporation	merged in 520	-	-
S3-110421	Supplemented description on how to handle the integrity verification failed message	ZTE Corporation	noted	-	-
S3-110423	Comparison of proposed solutions signals and compatibility aspects	ZTE Corporation	approved	-	-
S3-110424	Security threats analysis	ZTE Corporation	approved	-	-
S3-110425	UKM Solution 1 Cleanup	ZTE Corporation	approved	-	-
S3-110426	IWK with GERAN E-UTRAN for simplified forward security based solution	ZTE Corporation	approved with modifications	-	-
S3-110427	Updates of changes to messages of the simplified forward security base solution	ZTE Corporation	approved with modifications	-	-
S3-110428	Comparison table of changes to messages for 3 solutions	ZTE Corporation	approved with modifications	-	-
S3-110429	SRNS relocation without UE involvement for simplified forward security based solution	ZTE Corporation	approved	-	-
S3-110430	pCR on TR33.829- discussion paper of secure SRVCC	ZTE Corporation	noted	-	-
S3-110431	pCR on TR33.829 - e2e security solution for SRVCC	ZTE Corporation	sent for email approval	-	-
S3-110432	Optimization of implementing SSO_APS based on SIP Digest	ZTE Corporationï¼ŒChina Unicom	approved with modifications	-	-
S3-110433	Architecture for interworking with OpenID	ZTE Corporation, China Unicom	noted	-	-
S3-110434	Interworking message flow with OpenID	ZTE Corporation, China Unicom	noted	-	-
S3-110435	pCR to MTC Group Identifier	ZTE Corporation	withdrawn	-	-
S3-110436	pCR about general security requirements	ZTE Corporation	approved with modifications	-	S3-110557
S3-110437	pCR about secure connection	ZTE Corporation, China Unicom	approved	-	-
S3-110438	Location management in MTC Monitor	ZTE Corporation	noted	-	-
S3-110439	Security Issue - Broadcast message to a MTC group	ZTE Corporation	noted	-	-
S3-110440	security issue MTC device triggering requested by MTC server	ZTE Corporation	noted	-	-
S3-110441	pCR to MTC device Triggering Correction	China Unicom	approved	-	-
S3-110442	Replacing S3-110422_Clarification of the secure connection between RN and OAM server	ZTE Corporation	postponed to the next meeting	-	-

S3-110443	pCR to TR33.914 - interface consideration of Section 7.2.1	China Mobile,Nokia Corporation,Nokia Siemens Networks	approved with modifications	-	-
S3-110444	pCR to TR33.914 - solution update of Section 7.2.1	China Mobile	approved with modifications	-	-
S3-110445	pCR to TR33.914 - advantages of non-UICC base GBA in Section 7.2.2	China Mobile,Nokia Corporation,Nokia Siemens Networks	approved with modifications	-	-
S3-110446	HeNB security	China Mobile	noted	-	-
S3-110447	Improvement to solution 1 using protocol binding of SIP digest over TLS n TR 33.914	InterDigital	approved with modifications	-	-
S3-110448	Improvement to SIP digest SSO solution in section 7.3.2 with RP authentication details	InterDigital	approved with modifications	-	-
S3-110449	the confidentiality protection of the external interface	CATT	noted (covered by 517)	-	-
S3-110450	NDS enhancement - SCEP option for Certificate Enrolment to support backhaul security and network elements in general (R11	BT	noted	-	-
S3-110451	Alignment of RN security with RAN2/3 decision given in LS S3-110330 (R3-111034)	NTT docomo	merged in 520	-	-
S3-110452	Memory stress due to excessive updates of NAS security context	AT&T, Ericsson, Gemalto, Samsung, ST-Ericsson, Verizon Wireless	noted	-	-
S3-110453	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	revised	-	S3-110514
S3-110454	33.401 CR R9 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	revised	-	S3-110515
S3-110455	33.401 CR R10 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	revised	-	S3-110516
S3-110456	Discussion of MDT incoming LSs	NTT docomo	noted	-	-
S3-110457	draft Reply LS on MDT privacy	NTT docomo	revised	-	S3-

					110564
S3-110458	IANA MIKEY Assignments	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110459	Pre-Shared Key MIME Protection	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110460	KMS Based Immediate Messaging Protection	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110461	KMS Based Session-Based Messaging Protection	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110462	PWS Digital Signature Profile	Ericsson, ST-Ericsson	noted	-	-
S3-110463	LS on MDT configuration with user consent	R2-111714	noted	-	-
S3-110464	Reply to: Reply LS on Interaction with Trace for MDT (S5-111097 / S3-110203)	S5-111522	noted	-	-
S3-110465	draft LS on Security context mismatch in UMTS and GSM	Ericsson, ST-Ericsson	revised	-	S3-110544
S3-110466	Editorial corrections and clarifications to TR 33.859	Ericsson, ST-Ericsson	approved	-	-
S3-110467	Description of PUCI Function Communication	NEC Corporation	approved with modifications	-	-
S3-110468	PUCI Description	NEC Corporation	withdrawn	-	-
S3-110469	Security for direct interfaces between H(e)NBs	Nokia Corporation, Nokia Siemens Networks	postponed to the next meeting	-	-
S3-110470	TR 33.829: KMS conference group key update	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110471	TR 33.829: KMS conference group keying support	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110472	TR 33.829: Protection of event packages	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110473	TR 33.829: Conference system interfaces	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110474	TR 33.829: KMS Mutual authentication with MIKEY-TICKET (RFC 6043)	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110475	TR 33.829: KMS Update of allowed conference participants	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110476	TR 33.829: KMS Clarification conference call out	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110477	TR 33.829: KMS conference signalling	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110478	TR 33.829: KMS call diversion solution 2 update	Ericsson, ST-Ericsson	sent for email approval	-	-
S3-110479	Relation between 3GPP MTC security work and ETSI M2M	Vodafone	noted	-	-
S3-110480	Handling of maximum number of IKEv2 SAs	Ericsson, ST-Ericsson	noted	-	-
S3-110481	33.402 CR (R10): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	postponed to the next meeting	-	-
S3-110482	33.402 CR (R9): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	postponed to the next meeting	-	-
S3-110483	33.234 CR (R10): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	postponed to the next meeting	-	-
S3-110484	33.234 CR (R9): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	postponed to the next meeting	-	-
S3-110485	33.924 CR (R10): Alignment of HTTPS usage in GBA OpenID interworking	Ericsson, ST-Ericsson	revised	-	S3-110576
S3-110486	33.924 CR (R10): Relationship of identities in GBA OpenID interworking	Ericsson, ST-Ericsson	revised	-	S3-110574
S3-110487	OMA DM profile for MTC devices Configuration	China Mobile, Nokia Corporation, Nokia Siemens Networks	approved with modifications	-	-
S3-110488	Verification of the source of the device triggering message	China Unicom, Nokia Corporation, Nokia	noted	-	-

S3-110489	Clarifying enhancements to the MME in UTRAN KH study	Siemens Networks Qualcomm Incorporated	approved	-	-
S3-110490	Analysis of requirements in SA2 TR 23.888 related to external interface security	Ericsson, ST-Ericsson	noted	-	-
S3-110491	Potential security impact with Extended paging cycles	Ericsson, ST-Ericsson	noted	-	-
S3-110492	Analysis of CN and RN level key separation in UTRAN KH	Qualcomm Incorporated	approved with modifications	-	-
S3-110493	Restrict the use of a USIM to specific MEs/MTC Devices	Ericsson, ST-Ericsson	noted	-	-
S3-110494	Structure clarifications to SIP digest based GBA	Ericsson, ST-Ericsson	approved with modifications	-	-
S3-110495	33.110: Description in normative annex A of the key to be used in KDF	Gemalto, Verizon	revised	-	S3-110569
S3-110496	Confidentiality protection for MTC external interface	Ericsson, ST-Ericsson	revised	-	S3-110517
S3-110497	EPS algorithm negotiation during UTRAN to E-UTRAN handover	NEC Corporation	revised	-	S3-110530
S3-110500	Updating the system overview for TR 33.859	Ericsson, ST-Ericsson	approved with modifications	-	-
S3-110501	GBA Lite	Ericsson, ST-Ericsson, AT&T, Roger Wireless	noted	-	-
S3-110502	Security Enhancement for Usage of GBA from Browser	Ericsson, ST-Ericsson	noted	-	-
S3-110503	Security enhancements for usage of GBA from the browser	Nokia Corporation, Nokia Siemens Networks, China Mobile	revised	-	S3-110551
S3-110504	Usage of GBA with the Web	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110505	Types of credentials for the SSO study	Ericsson, ST-Ericsson	noted	-	-
S3-110506	Modification of security context storage rate on the USIM	Nokia Corporation, Nokia Siemens Networks	sent for email discussion	-	-
S3-110507	Relation of SSO TR to other work in 3GPP	Ericsson, ST-Ericsson	approved	-	-
S3-110508	RN certificate handling simplification	NTT docomo	postponed to the next meeting	-	-
S3-110509	Comments on S3-110347, 'P-CR Generic Terminal Requirements for using UICC credentials for SSO from a browser'	Alcatel-Lucent, AT&T	noted	-	-
S3-110510	Guidelines for SA3 Delegates v020	MCC	noted	-	-
S3-110511	Comments to GBA Lite (S3-110501)	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110512	Comments to Discussion of MDT privacy requirements (S3-110456)	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110513	Comments to pCR to TR 33.sso Section 8, Solutions (S3-110306)	Nokia Corporation, Nokia Siemens Networks	noted	-	-
S3-110514	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE	revised	S3-110453	S3-110525

		Corporation			
S3-110515	33.401 CR R9 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	revised	S3-110454	S3-110527
S3-110516	33.401 CR R10 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	revised	S3-110455	S3-110528
S3-110517	Confidentiality protection for MTC external interface	Ericsson, ST-Ericsson	approved	S3-110496	-
S3-110518	Comments on S3-110421 Supplemented description on how to handle the integrity verification failed message	Nokia Siemens Networks	noted	-	-
S3-110519	Comments by Nokia Siemens Networks on S3-110442 Clarification of the secure connection between RN and OAM server	Nokia Siemens Networks	noted	-	-
S3-110520	Proposed merger of S3-110396, 420, 451 Corrections to communication between MME and DeNB for relay nodes	Nokia Siemens Networks	revised	-	S3-110533
S3-110521	Comments on S3-110508 RN certificate handling simplification	Nokia Siemens Networks	noted	-	-
S3-110522	COMMENTS on Methodology for the evaluation of UTRAN security enhancements	Ericsson, ST-Ericsson, ZTE Corporation	noted	-	-
S3-110523	Comment on'H(e)NB. Security of direct interfaces' (S3-110305)	Nokia Siemens Networks	noted	-	-
S3-110524	Comments on S3-110350 Privacy Considerations in Management / Area MDT	NEC Corporation	noted	-	-
S3-110525	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	revised	S3-110514	S3-110526
S3-110526	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE,	agreed	S3-110525	-

		Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation			
S3-110527	33.401 CR R9 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	agreed	S3-110515	-
S3-110528	33.401 CR R10 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	agreed	S3-110516	-
S3-110529	Reply to: LS on excessive updates of NAS security context	Ericsson	approved	-	-
S3-110530	EPS algorithm negotiation during UTRAN to E-UTRAN handover	NEC Corporation	agreed	S3-110497	-
S3-110531	LS on Handling of maximum number of IKEv2 Sas	Ericsson	approved	-	-
S3-110532	Reply LS to COM13-LS147 Response liaison statement on OpenID interworking with AKA	Alcatel-Lucent	withdrawn	-	-
S3-110533	Corrections to communication between MME and DeNB for relay nodes	Nokia Siemens Networks, China Mobile, Gemalto, NTT Docomo, ZTE	agreed	S3-110520	-
S3-110534	Corrective text for undefined wording - autonomous validation of RN platform	InterDigital, China Mobile, Nokia Siemens Networks	agreed	S3-110311	-
S3-110535	Resolution of Editor's Notes for PDPC integrity for Relay Nodes	Nokia Siemens Networks	agreed	S3-110395	-
S3-110536	CR-Detailed binding of RN and UICC	Huawei, HiSilicon	agreed	S3-110352	-
S3-110537	Specification of secure channel profiles and certificates used for Relay nodes (RNs) and UICC (USIM-RN)	Nokia Siemens Networks	agreed	S3-110397	-
S3-110538	Correction on communication outside secure channel for Relay Node security procedures	China Mobile, Gemalto, InterDigital Communications, Nokia Siemens Networks, Sagem-Orga	agreed	S3-110400	-
S3-110539	Clarification of certificate and subscription handling	China Mobile,Nokia Siemens Networks, Nokia Corporation	agreed	S3-110378	-
S3-110540	Attack description concerning CRL handling in RN solution	NTT Docomo	noted	-	-

S3-110541	CR-Clarification on initial attach procedure for PSK case	Huawei, HiSilicon	agreed	S3-110354	-
S3-110542	Resolution of Editor's Notes for Relay Node security procedures	Nokia Siemens Networks, China Mobile	agreed	S3-110398	-
S3-110543	Corrections and Clarifications for Relay Node security procedures	Nokia Siemens Networks, Gemalto	agreed	S3-110399	-
S3-110544	LS on Security context mismatch in UMTS and GSM	Ericsson, ST-Ericsson	approved	S3-110465	-
S3-110545	LS on CSG security for H(e)NB	Alcatel-Lucent, Alcatel-Lucent Shanghai Bell	approved	S3-110393	-
S3-110546	LS on Removal of Hosting Party Authentication	Qualcomm Incorporated	approved	-	-
S3-110547	Security mechanism for H(e)NB no-IPsec usage option [Rel-9]	Samsung	agreed	S3-110385	-
S3-110548	Security mechanism for H(e)NB no-IPsec usage option [Rel-10]	Samsung	agreed	S3-110386	-
S3-110549	Security mechanism for H(e)NB no-IPsec usage option [Rel-11]	Samsung	agreed	S3-110387	-
S3-110550	New version of SPUCI TR	NEC (Rapporteur)	agreed	-	-
S3-110551	Security enhancements for usage of GBA from the browser	Nokia Corporation, Nokia Siemens Networks, China Mobile	approved	S3-110503	-
S3-110552	Void	Void	withdrawn	-	-
S3-110553	CR - A5/3 support in GSM	Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera	agreed	S3-110389	-
S3-110554	CR - A5/3 and A5/4 support in GSM	Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera	agreed	-	-
S3-110555	Update of SIMTC WID	Samsung	approved	S3-110392	-
S3-110556	Reply to: LS on MTC USIM requirements for Release 10	Ericsson	approved	-	-
S3-110557	New version of MTC Security Aspects TR	Samsung	agreed	-	-
S3-110558	LS to on potential co-operation between 3GPP work on MTC security and ETSI M2M	Vodafone	approved	-	-
S3-110559	Clarification for MTC device triggering	Huawei, HiSilicon	approved with modifications	S3-110362	-
S3-110560	pCR to Solution 1 Triggering	China Mobile,ZTE, Interdigital	approved with modifications	S3-110377	-
S3-110561	LS to SA2 on confidentiality protection for MTC external device	Ericsson	approved	-	-
S3-110562	LS on potential security impact with Extended paging cycles	Ericsson	sent for email approval	-	-
S3-110563	LS on Security mechanism for H(e)NB no-IPsec usage option	CMCC	approved	-	-
S3-110564	Reply to: Liaison statement on user consent in area or management based MDT activation	NTT Docomo	revised	-	S3-110575
S3-110565	New version of PWS security living document	Huawei	approved	-	-
S3-110566	Security features of PWS	Huawei, HiSilicon	approved	S3-110365	-
S3-110567	Removal of mandatory support for HTTPS in CMP transport-R9	Huawei, HiSilicon, Nokia Corporation, Nokia Siemens Networks	agreed	S3-110367	-
S3-110568	Removal of mandatory support for HTTPS in CMP transport-R10	Huawei, HiSilicon,Nokia Corporation, Nokia Siemens Networks	agreed	S3-110368	-
S3-110569	33.110: Description in normative annex A of the key to be used in KDF	Gemalto, Verizon	agreed	S3-110495	-
S3-110570	33.110: Description in normative annex A of the key to be used in KDF	Gemalto, Verizon	agreed	-	-

S3-110571	New version of UKH TR	Ericsson (Rapporteur)	sent for email approval	-	-
S3-110572	Reply LS on Requirements and Architecture issues of PSS service	Ericsson	approved	-	-
S3-110573	Reply to: LS on LI requirements related to encryption	BT	approved	-	-
S3-110574	33.924 CR (R10): Relationship of identities in GBA OpenID interworking	Ericsson, ST-Ericsson	agreed	S3-110486	-
S3-110575	Reply to: Liaison statement on user consent in area or management based MDT activation	NTT Docomo	approved	S3-110564	-
S3-110576	33.924 CR (R9): Correction of UA security protocol identifier in GBA - OpenID interworking	Ericsson, ST-Ericsson	agreed	S3-110485	-
S3-110577	33.924 CR (R9): Correction of UA security protocol identifier in GBA - OpenID interworking	Ericsson, ST-Ericsson	agreed	S3-110485	-
S3-110578	New version of TR on IMS Media Security	Vodafone	sent for email approval	-	-
S3-110579	LS on clarification of type(s) of operator-controlled SSO credentials	Ericsson	sent for email approval	-	-
S3-110580	New version of TR on Study on Security aspects of Integration of Single Sign-On (SSO) frameworks with 3GPP networks	Ericsson	sent for email approval	-	-
S3-110581	New version of TR on Study on Single Sign On (SSO) Application Security for IMS - based on SIP Digest	Nokia	sent for email approval	-	-
S3-110582	SA3 Meeting Calendar	SA3 Secretary, SA3 Chairman	approved	S3-110304	-
S3-110583	Merger of 373, 443, 444, 445, 494	Nokia	noted	-	-

Annex B: List of change requests

Document	Title	Source	Spec	CR	Rev	Rel	Cat	WI	Decision
S3-110506	Modification of security context storage rate on the USIM	Nokia Corporation, Nokia Siemens Networks	33.102	CRNum	-	Rel-11	F	TEI11	sent for email discussion
S3-110495	33.110: Description in normative annex A of the key to be used in KDF	Gemalto, Verizon	33.110	0018	-	Rel-9	F	KeyEstUTerm	revised
S3-110569	33.110: Description in normative annex A of the key to be used in KDF	Gemalto, Verizon	33.110	0018	1	Rel-9	F	KeyEstUTerm	agreed
S3-110570	33.110: Description in normative annex A of the key to be used in KDF	Gemalto, Verizon	33.110	0019	-	Rel-11	A	KeyEstUTerm	agreed
S3-110381	[33.210] Clarification of algorithm names and DH group usage in IKEv2	Nokia Corporation, Nokia Siemens Networks	33.210	39	-	Rel-11	F	TEI11	agreed
S3-110382	[33.210, rel-10] Correction of Iuh/Iurh security	Nokia Corporation, Nokia Siemens Networks	33.210	40	-	Rel-10	F	TEI10	agreed
S3-110383	[33.210, rel-11] Correction of Iuh/Iurh security	Nokia Corporation, Nokia Siemens Networks	33.210	41	-	Rel-11	A	TEI10	agreed
S3-110483	33.234 CR (R10): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	33.234	109	-	Rel-10	A	TEI9	postponed to the next meeting
S3-110484	33.234 CR (R9): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	33.234	110	-	Rel-9	F	TEI9	postponed to the next meeting
S3-110367	Removal of mandatory support for HTTPS in CMP transport-R9	Huawei, HiSilicon, Nokia Corporation, Nokia Siemens Networks	33.310	48	-	Rel-9	F	NDS_Backhaul	revised
S3-110567	Removal of mandatory support for HTTPS in CMP transport-R9	Huawei, HiSilicon, Nokia Corporation, Nokia Siemens Networks	33.310	48	1	Rel-9	F	NDS_Backhaul	agreed
S3-110368	Removal of mandatory support for HTTPS in CMP transport-R10	Huawei, HiSilicon,Nokia Corporation, Nokia Siemens Networks	33.310	49	-	Rel-10	A	NDS_Backhaul	revised
S3-110568	Removal of mandatory support for HTTPS in CMP transport-R10	Huawei, HiSilicon,Nokia Corporation, Nokia Siemens Networks	33.310	49	1	Rel-10	A	NDS_Backhaul	agreed
S3-110369	CMPv2 message format	Huawei, HiSilicon	33.310	50	-	Rel-11	F	NDS_Backhaul	noted
S3-110379	Correction of reference for key usage bit in TLS certificate and some editorials	Nokia Corporation, Nokia Siemens Networks	33.310	51	-	Rel-10	F	TEI10	agreed

S3-110380	Correction on CRL distribution point for vendor root CA certificates	Nokia Corporation, Nokia Siemens Networks	33.310	52	-	Rel-10	F	TEI10	agreed
S3-110450	NDS enhancement - SCEP option for Certificate Enrolment to support backhaul security and network elements in general (R11	BT	33.310	CRNum	-	Rel-11	B	Backhaul security	noted
S3-110469	Security for direct interfaces between H(e)NBs	Nokia Corporation, Nokia Siemens Networks	33.320	58	1	Rel-11	B	HNB_mob_Sec	postponed to the next meeting
S3-110312	Removal of Hosting Party Authentication, R9	Qualcomm Incorporated	33.320	62	-	Rel-9	F	EHNB-Sec	noted
S3-110313	Removal of Hosting Party Authentication, R10	Qualcomm Incorporated	33.320	63	-	Rel-10	F	EHNB-Sec	noted
S3-110314	Location Verification Correction, R9	Qualcomm Incorporated	33.320	64	-	Rel-9	F	EHNB-Sec	withdrawn
S3-110315	Location Verification Correction, R10	Qualcomm Incorporated	33.320	65	-	Rel-10	F	EHNB-Sec	withdrawn
S3-110316	Location Verification Correction, R11	Qualcomm Incorporated	33.320	66	-	Rel-11	F	EHNB-Sec	withdrawn
S3-110386	Security mechanism for H(e)NB no-IPsec usage option [Rel-10]	Samsung	33.320	66	-	Rel-11	A	EHNB-Sec	revised
S3-110548	Security mechanism for H(e)NB no-IPsec usage option [Rel-10]	Samsung	33.320	66	1	Rel-10	A	EHNB-Sec	agreed
S3-110385	Security mechanism for H(e)NB no-IPsec usage option [Rel-9]	Samsung	33.320	67	-	Rel-9	F	EHNB-Sec	revised
S3-110387	Security mechanism for H(e)NB no-IPsec usage option [Rel-11]	Samsung	33.320	67	-	Rel-11	A	EHNB-Sec	revised
S3-110547	Security mechanism for H(e)NB no-IPsec usage option [Rel-9]	Samsung	33.320	67	1	Rel-9	F	EHNB-Sec	agreed
S3-110549	Security mechanism for H(e)NB no-IPsec usage option [Rel-11]	Samsung	33.320	67	1	Rel-11	A	EHNB-Sec	agreed
S3-110390	H(e)NB-LGW Remote IP Address Assignment [Rel-10]	Samsung, Qualcomm	33.320	70	-	Rel-10	F	LIPA_SIPTO	noted
S3-110391	H(e)NB-LGW Remote IP Address Assignment [Rel-11]	Samsung, Qualcomm	33.320	71	-	Rel-11	A	LIPA_SIPTO	noted
S3-110451	Alignment of RN security with RAN2/3 decision given in LS S3-110330 (R3-111034)	NTT docomo	33.401	-	-	Rel-10	F	LTE_Relay-Sec	merged in 520
S3-110497	EPS algorithm negotiation during UTRAN to E-UTRAN handover	NEC Corporation	33.401	428	-	Rel-11	B	SAES	revised
S3-110530	EPS algorithm negotiation during UTRAN to E-	NEC Corporation	33.401	428	1	Rel-11	B	TEI11	agreed

	UTRAN handover								
S3-110311	Corrective text for undefined wording - autonomous validation of RN platform	InterDigital, China Mobile, Nokia Siemens Networks	33.401	440	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110534	Corrective text for undefined wording - autonomous validation of RN platform	InterDigital, China Mobile, Nokia Siemens Networks	33.401	440	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110420	Correction of the RN attach procedure	ZTE Corporation	33.401	441	-	Rel-10	F	LTE_Relay-Sec	merged in 520
S3-110421	Supplemented description on how to handle the integrity verification failed message	ZTE Corporation	33.401	442	-	Rel-10	F	LTE_Relay-Sec	noted
S3-110442	Replacing S3-110422_Clarification of the secure connection between RN and OAM server	ZTE Corporation	33.401	443	-	Rel-10	F	LTE_Relay-Sec	postponed to the next meeting
S3-110352	CR-Detailed binding of RN and UICC	Huawei, HiSilicon	33.401	444	-	Rel-10	F	LTE_RELAY_SEC	revised
S3-110536	CR-Detailed binding of RN and UICC	Huawei, HiSilicon	33.401	444	1	Rel-10	F	LTE_RELAY_SEC	agreed
S3-110354	CR-Clarification on initial attach procedure for PSK case	Huawei, HiSilicon	33.401	445	-	Rel-10	F	LTE_RELAY_SEC	revised
S3-110541	CR-Clarification on initial attach procedure for PSK case	Huawei, HiSilicon	33.401	445	1	Rel-10	F	LTE_RELAY_SEC	agreed
S3-110418	CR-Security handling for relay related UE handover	Huawei, HiSilicon	33.401	446	-	Rel-10	F	LTE_RELAY_SEC	noted
S3-110358	CR-Algorithm negotiation on Un interface	Huawei, HiSilicon	33.401	447	-	Rel-10	F	LTE_RELAY_SEC	withdrawn
S3-110378	Clarification of certificate and subscription handling	China Mobile,Nokia Siemens Networks, Nokia Corporation	33.401	448	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110539	Clarification of certificate and subscription handling	China Mobile,Nokia Siemens Networks, Nokia Corporation	33.401	448	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110395	Resolution of Editor's Notes for PDPC integrity for Relay Nodes	Nokia Siemens Networks	33.401	449	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110535	Resolution of Editor's Notes for PDPC integrity for Relay Nodes	Nokia Siemens Networks	33.401	449	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110396	Corrections to communication between MME and DeNB for relay nodes	Nokia Siemens Networks, China Mobile, Gemalto	33.401	450	-	Rel-10	F	LTE_Relay-Sec	merged in 520
S3-110520	Proposed merger of S3-110396, 420, 451 Corrections to	Nokia Siemens Networks	33.401	450	1	Rel-10	F	LTE_Relay-Sec	revised

	communication between MME and DeNB for relay nodes								
S3-110397	Specification of secure channel profiles and certificates used for Relay nodes (RNs) and UICC (USIM-RN)	Nokia Siemens Networks	33.401	451	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110537	Specification of secure channel profiles and certificates used for Relay nodes (RNs) and UICC (USIM-RN)	Nokia Siemens Networks	33.401	451	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110398	Resolution of Editor's Notes for Relay Node security procedures	Nokia Siemens Networks, China Mobile	33.401	452	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110542	Resolution of Editor's Notes for Relay Node security procedures	Nokia Siemens Networks, China Mobile	33.401	452	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110399	Corrections and Clarifications for Relay Node security procedures	Nokia Siemens Networks, Gemalto	33.401	453	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110543	Corrections and Clarifications for Relay Node security procedures	Nokia Siemens Networks, Gemalto	33.401	453	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110400	Correction on communication outside secure channel for Relay Node security procedures	China Mobile, Gemalto, InterDigital Communications, Nokia Siemens Networks, Sagem-Orga	33.401	454	-	Rel-10	F	LTE_Relay-Sec	revised
S3-110538	Correction on communication outside secure channel for Relay Node security procedures	China Mobile, Gemalto, InterDigital Communications, Nokia Siemens Networks, Sagem-Orga	33.401	454	1	Rel-10	F	LTE_Relay-Sec	agreed
S3-110508	RN certificate handling simplification	NTT docomo	33.401	456	-	Rel-10	F	LTE_Relay-Sec	postponed to the next meeting
S3-110453	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless,	33.401	457	-	Rel-8	F	TEI11	revised

S3-110514	33.401 CR R8 Modification of security context storage rate	Vodafone, ZTE Corporation Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	457	1	Rel-8	F	TEI11	revised
S3-110525	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	457	2	Rel-8	F	TEI8	revised
S3-110526	33.401 CR R8 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	457	3	Rel-8	F	TEI8	agreed
S3-110454	33.401 CR R9 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola	33.401	458	-	Rel-9	A	TEI11	revised

		Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation								
S3-110515	33.401 CR R9 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	458	1	Rel-9	A	TEI11		revised
S3-110527	33.401 CR R9 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	458	2	Rel-9	A	TEI8		agreed
S3-110455	33.401 CR R10 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson,	33.401	459	-	Rel-10	A	TEI11		revised

S3-110516	33.401 CR R10 Modification of security context storage rate	Verizon Wireless, Vodafone, ZTE Corporation Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	459	1	Rel-10	A	TEI11	revised
S3-110528	33.401 CR R10 Modification of security context storage rate	Alcatel-Lucent, AT&T, Cisco, Ericsson, Gemalto, Giesecke and Devrient, HTC, LGE, Motorola Mobility, Nokia Corporation, Nokia Siemens Networks, Research In Motion UK Limited, Samsung, ST-Ericsson, Verizon Wireless, Vodafone, ZTE Corporation	33.401	459	2	Rel-10	A	TEI8	agreed
S3-110533	Corrections to communication between MME and DeNB for relay nodes	Nokia Siemens Networks, China Mobile, Gemalto, NTT Docomo, ZTE	33.401	460	-	Rel-10	F	LTE_Relay-Sec	agreed
S3-110481	33.402 CR (R10): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	33.402	96	-	Rel-10	A	TEI9	postponed to the next meeting
S3-110482	33.402 CR (R9): Removal of maximum number of IKEv2 SA limit	Ericsson, ST-Ericsson	33.402	97	-	Rel-9	F	TEI9	postponed to the next meeting
S3-110349	Correction of Ua security protocol identifier for OpenID-GBA Interworking	Nokia Corporation, Nokia Siemens Networks	33.924	16	-	Rel-9	F	TEI9	merged in S3-110576
S3-110485	33.924 CR (R10): Alignment of HTTPS usage in GBA OpenID interworking	Ericsson, ST-Ericsson	33.924	17	-	Rel-10	F	TEI10	revised
S3-110486	33.924 CR (R10): Relationship of identities in GBA	Ericsson, ST-Ericsson	33.924	18	-	Rel-10	F	TEI10	revised

S3-110574	OpenID interworking 33.924 CR (R10): Relationship of identities in GBA	Ericsson, ST-Ericsson	33.924	18	1	Rel-10	F	TEI10	agreed
S3-110576	OpenID interworking 33.924 CR (R9): Correction of UA security protocol identifier in GBA -	Ericsson, ST-Ericsson	33.924	19	-	Rel-9	F	TEI9	agreed
S3-110577	OpenID interworking 33.924 CR (R9): Correction of UA security protocol identifier in GBA -	Ericsson, ST-Ericsson	33.924	20	-	Rel-9	A	TEI9	agreed
S3-110389	OpenID interworking CR - A5/3 and A5/4 support in GSM	Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera	43.020	0027	-	Rel-10	B	TEI10	revised
S3-110553	CR - A5/3 support in GSM	Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera	43.020	0027	1	Rel-10	F	TEI10	agreed
S3-110554	CR - A5/3 and A5/4 support in GSM	Orange, Vodafone, KPN, Deutsche Telekom, TeliaSonera	43.020	0028	-	Rel-10	B	TEI10	agreed

Annex C: Lists of liaisons

C1: Incoming liaison statements

Document	Title	From	Decision	Reply in
S3-110317	Response LS on Security and Authentication in UDC	C4-102710	noted	
S3-110318	Reply LS on review of MDT design and reply LS on Security Issues with Logged MDT	S5-110529	noted	
S3-110319	Encryption algorithms for UDC	SAGE-10-09	noted	
S3-110320	Reply LS on MDT user involvement (S5-110367 / R2-110699)	S5-110482	noted	
S3-110321	LS reply on OAM architecture aspects for RNs (S5-110067 / R3-102541)	S5-110546	noted	
S3-110322	Response liaison statement to 3GPP TSG SA on OpenID interworking with AKA	COM13-LS147	postponed to the next meeting	S3-110532
S3-110323	Answer to Liaison Statement regarding 3GPP SSO integration without GBA	OMA-LS_896-OMA_ARC_to_3GPP_SA3_OpenID-20110209-A	postponed to the next meeting	
S3-110324	LS on LI requirements related to encryption	SA3LI11_058r1	replied to	S3-110573
S3-110325	Reply LS on LCLS optional functionality in BSS	SA3LI11_059r1	noted	
S3-110326	Reply LS on Relay Node OAM System Discovery	R3-110968	noted	
S3-110327	LS on MTC USIM requirements for Release 10	C1-111155	replied to	
S3-110328	Reply LS for MDT	S1-110172	noted	
S3-110329	Reply LS on OAM architecture aspects for RNs	R3-110970	noted	
S3-110330	Reply LS on Security for LTE relay nodes	R3-111034	noted	
S3-110331	LS on PWS security	C1-111150	noted	
S3-110332	LS on maximum value of extended wait timer	C1-111500	noted	
S3-110333	LS on partial success of Write Replace Warning Request for ETWS	R3-111084	noted	
S3-110334	Reply LS on Simultaneous registration of a single private identity from different UEs	S2-111153	noted	
S3-110335	LS on MTC USIM requirements for Release 10	S1-110422	replied to	
S3-110336	LS on Release 10 NIMTC Work	GP-110382	noted	
S3-110337	Reply LS on Cell Broadcast Service for MOCN Shared Network	S2-111272	noted	
S3-110338	Reply LS on Liaison Statement on security issues of PSS service	S4-110335	noted	
S3-110339	Reply LS on Requirements and Architecture issues of PSS service	S1-110175	replied to	S3-110572
S3-110340	LS on User consent indication for MDT	R3-110931	noted	
S3-110341	LS on excessive updates of NAS security context	C6-110184	replied to	S3-110529
S3-110342	LS on additional considerations of Relay Nodes in the LTE-Advanced material for Rec. ITU-R M.[IMT.RSPEC] to be submitted to ITU-R WP5D#10 (6-13 April, 2011)	RP-110006	noted	
S3-110343	Reply LS on MTC Planning and Prioritization	SP-110218	noted	
S3-110344	Liaison statement on user consent in	SP-110230	replied to	S3-

	area or management based MDT activation			110575
S3-110344	Liaison statement on user consent in area or management based MDT activation	SP-110230	replied to	S3-110564
S3-110345	LS on Network Sharing	SP-110234	noted	
S3-110346	LS on MDT User consent handling	S5-111525	noted	
S3-110463	LS on MDT configuration with user consent	R2-111714	noted	
S3-110464	Reply to: Reply LS on Interaction with Trace for MDT (S5-111097 / S3-110203)	S5-111522	noted	

C2: Outgoing liaison statements

Document	Title	To	Cc	reply to i/c LS
S3-110529	Reply to: LS on excessive updates of NAS security context	C6-110184	-	S3-110341
S3-110531	LS on Handling of maximum number of IKEv2 Sas	SA2, CT1	-	-
S3-110544	LS on Security context mismatch in UMTS and GSM	-	-	-
S3-110545	LS on CSG security for H(e)NB	-	-	-
S3-110546	LS on Removal of Hosting Party Authentication	-	-	-
S3-110556	Reply to: LS on MTC USIM requirements for Release 10	C1-111155, S1-110422	-	S3-110327, S3-110335
S3-110558	LS to on potential co-operation between 3GPP work on MTC security and ETSI M2M	ETSI M2M	-	
S3-110561	LS to SA2 on confidentiality protection for MTC external device	-	-	
S3-110563	LS on Security mechanism for H(e)NB no-IPsec usage option	-	-	
S3-110572	Reply LS on Requirements and Architecture issues of PSS service	S1-110175	-	S3-110339
S3-110573	Reply to: LS on LI requirements related to encryption	SA3LI11_058r1	-	S3-110324
S3-110575	Reply to: Liaison statement on user consent in area or management based MDT activation	SP-110230	-	S3-110344

C3: Outgoing liaison statements under email approval

Tdoc	Title	Agenda
S3-110562	LS on potential security impact with Extended paging cycles	7.9
S3-110579	LS on clarification of type(s) of operator-controlled SSO credentials	8.5

Annex D: List of agreed/approved new and revised Work Items

Document	Title	Source	new/revised
S3-110551	Security enhancements for usage of GBA from the browser	Nokia Corporation, Nokia Siemens Networks, China Mobile	New WID
S3-110555	Update of SIMTC WID	Samsung	revised WID

Annex E: List of draft Technical Specifications and Reports

The following TSs/TRs were agreed to be sent for information/approval to SA:

Document	Spec	vers	Doc title
S3-110581	-	..	New version of TR on Study on Single Sign On (SSO) Application Security for IMS - based on SIP Digest (for SA information)

Annex F: List of action items

Meeting/Number	Agenda item	Document	Details	Responsible	Due by
S3-63/1	4	S3-110345	check specifications to see if there are any existing features where network sharing is not supported and report back	Rapporteurs	

Annex G: List of email approvals

The following contributions under agenda item 8.3 were sent for email approval:

Tdoc	Title	Source	Status
S3-110309	pCR to TR 33.mps Services for user groups with high security requirements	Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell	ongoing
S3-110310	Clarification of requirements and capabilities for clause 7.1	Alcatel Lucent, AT&T, Alcatel-Lucent Shanghai Bell	ongoing
S3-110409	Pseudo CR to TR 33.829: Impact of Communications Diversion (CDIV) on peer identification	Nokia Corporation, Nokia Siemens Networks	ongoing
S3-110410	Pseudo CR to TR 33.829: More detailed discussion of the SDES solution for CDIV	Nokia Corporation, Nokia Siemens Networks	ongoing
S3-110411	Pseudo CR for TR 33.829: Security Policies for Conferencing	Nokia Corporation, Nokia Siemens Networks	ongoing
S3-110412	Pseudo CR for TR 33.829: Enhanced Description of the SDES Based Solution for Conferencing	Nokia Corporation, Nokia Siemens Networks	ongoing
S3-110413	Pseudo CR for TR 33.829: Minor Changes to the Messaging Description	Nokia Corporation, Nokia Siemens Networks	ongoing
S3-110414	Pseudo CR for TR 33.829: Solution Proposal for Messaging	Nokia Corporation, Nokia Siemens Networks	ongoing
S3-110431	pCR on TR33.829 - e2e security solution for SRVCC	ZTE Corporation	ongoing
S3-110458	IANA MIKEY Assignments	Ericsson, ST-Ericsson	ongoing
S3-110459	Pre-Shared Key MIME Protection	Ericsson, ST-Ericsson	ongoing
S3-110460	KMS Based Immediate Messaging Protection	Ericsson, ST-Ericsson	ongoing
S3-110461	KMS Based Session-Based Messaging Protection	Ericsson, ST-Ericsson	ongoing
S3-110470	TR 33.829: KMS conference group key update	Ericsson, ST-Ericsson	ongoing
S3-110471	TR 33.829: KMS conference group keying support	Ericsson, ST-Ericsson	ongoing
S3-110472	TR 33.829: Protection of event packages	Ericsson, ST-Ericsson	ongoing
S3-110473	TR 33.829: Conference system interfaces	Ericsson, ST-Ericsson	ongoing
S3-110474	TR 33.829: KMS Mutual authentication with MIKEY-TICKET (RFC 6043)	Ericsson, ST-Ericsson	ongoing
S3-110475	TR 33.829: KMS Update of allowed conference participants	Ericsson, ST-Ericsson	ongoing
S3-110476	TR 33.829: KMS Clarification conference call out	Ericsson, ST-Ericsson	ongoing
S3-110477	TR 33.829: KMS conference signalling	Ericsson, ST-Ericsson	ongoing
S3-110478	TR 33.829: KMS call diversion solution 2 update	Ericsson, ST-Ericsson	ongoing

S3-110578 New version of TR on IMS Media Security Vodafone

S3-110578 was revised and email approved as S3-110584.

The following contributions under other agenda items were sent for email approval:

S3-110562	LS on potential security impact with Extended paging cycles	Ericsson	o/g LS	withdrawn
S3-110571	New version of UKH TR	Ericsson (Rapporteur)	draft TS/TR	agreed
S3-110579	LS on clarification of type(s) of operator-controlled SSO credentials	Ericsson	o/g LS	approved
S3-110580	New version of TR on Study on Security aspects of Integration of Single Sign-On (SSO) frameworks with 3GPP networks	Ericsson	draft TS/TR	agreed
S3-110581	New version of TR on Study on Single Sign On (SSO) Application Security for IMS - based on SIP Digest	Nokia	TS/TR for info	agreed

Annex H: List of participants

Name	Representing	Status-Partner	Ctry
Aldén, Magnus (Dr.)	TeliaSonera AB	3GPPMEMBER (ETSI)	SE
Bi, Xiaoyu (Ms.)	HuaWei Technologies Co., Ltd	3GPPMEMBER (ATIS)	JP
Blanchard, Colin (Mr.)	BT Group Plc	3GPPMEMBER (ETSI)	GB
Blom, Rolf (Dr.)	Ericsson Inc.	3GPPMEMBER (ATIS)	SE
Brusilovsky, Alec (Mr.)	Alcatel-Lucent	3GPPMEMBER (ETSI)	US
Cakulev, Violeta (Mrs.)	Alcatel-Lucent Telecom Ltd	3GPPMEMBER (ETSI)	US
Canciu, Nick (Mr.)	Rogers Wireless Inc.	3GPPMEMBER (ATIS)	CA
Castagno, Mauro (Mr.)	TELECOM ITALIA S.p.A.	3GPPMEMBER (ETSI)	IT
Cha, Inhyok (Dr.)	INTERDIGITAL COMMUNICATIONS	3GPPMEMBER (ETSI)	US
Chen, Jing (Mr.)	HUAWEI TECHNOLOGIES Co. Ltd.	3GPPMEMBER (ETSI)	CN
Dolly, Martin (Mr.)	AT&T	3GPPMEMBER (ATIS)	US
Feng, Cathy (Miss)	ZTE Corporation	3GPPMEMBER (ETSI)	CN
Fransen, Frank (Mr.)	KPN N.V.	3GPPMEMBER (ETSI)	NL
Gao, Feng (Ms.)	ZTE Corporation	3GPPMEMBER (ETSI)	CN
He, dony (Mr.)	HuaWei Technologies Co., Ltd	3GPPMEMBER (CCSA)	CN
Hernandez, Pedro (Mr.)	GIESECKE & DEVRIENT GmbH	3GPPMEMBER (ETSI)	ES
Holtmanns, Silke (Dr.)	NOKIA Corporation	3GPPMEMBER (ETSI)	FI
Horn, Guenther (Dr.)	Nokia Siemens Networks	3GPPMEMBER (ETSI)	DE
Howard, Peter (Mr.)	VODAFONE Group Plc	3GPPMEMBER (ETSI)	GB
Huang, Bojian (Mr.)	HuaWei Technologies Co., Ltd	3GPPMEMBER (CCSA)	CN
Jia, Jia (Ms.)	China Unicom	3GPPMEMBER (CCSA)	CN
Jing, Yejing (Ms.)	CATT	3GPPMEMBER (CCSA)	CN
Kaufmann, Tobias (Mr.)	BMWi	3GPPMEMBER (ETSI)	DE
Krainioukov, Oleg (Mr.)	Sagem Orga GmbH	3GPPMEMBER (ETSI)	DE
Kuang, Xiaoxuan (Miss)	CATR	3GPPMEMBER (CCSA)	CN
Leadbeater, Alex (Mr.)	BT Group Plc	3GPPMEMBER (ETSI)	GB
Lehtovirta, Vesa (Mr.)	Nanjing Ericsson Panda Com Ltd	3GPPMEMBER (CCSA)	US
Li, Yang (Mr.)	ZTE Corporation	3GPPMEMBER (ETSI)	CN
Liu, Qiuyuan (Dr.)	Juniper Networks	3GPPMEMBER (ETSI)	US
Luft, Achim (Mr.)	Intel Corporation (UK) Ltd	3GPPMEMBER (ETSI)	DE
Michau, Benoit (Mr.)	ORANGE SA	3GPPMEMBER (ETSI)	FR
Moeller, Wolf-Dietrich (Dr.)	Nokia Siemens Networks Oy	3GPPMEMBER (ETSI)	DE
Norrman, Karl (Mr.)	Nippon Ericsson K.K.	3GPPMEMBER (ARIB)	SE
Palanigounder, Anand (Mr.)	QUALCOMM CDMA Technologies	3GPPMEMBER (ETSI)	US
Pauliac, Mireille (Miss)	Gemalto N.V.	3GPPMEMBER (ETSI)	FR
Pildush, Galina (Dr.)	Juniper Networks	3GPPMEMBER (ETSI)	US
Prasad, Anand (Dr.)	NEC Corporation	3GPPMEMBER (ARIB)	JP
Qi, Minpeng (Mr.)	China Mobile Com. Corporation	3GPPMEMBER (CCSA)	CN
Rajadurai, Rajavelsamy (Mr.)	SAMSUNG Electronics Co.	3GPPMEMBER (ARIB)	IN
Rosenberg, Brian (Mr.)	Qualcomm Incorporated	3GPPMEMBER (ATIS)	US
Sahlin, Bengt (Mr.)	Telefon AB LM Ericsson	3GPPMEMBER (ETSI)	SE
Schroeder, Stefan (Mr.)	Deutsche Telekom AG	3GPPMEMBER (ETSI)	DE
Tian, Tian (Miss)	ZTE Corporation	3GPPMEMBER (ETSI)	CN
Wong, Marcus (Mr.)	Huawei Technologies (UK)	3GPPMEMBER (ETSI)	US
Xia, ZhengXue (Mr.)	ZTE Corporation	3GPPMEMBER (CCSA)	CN
Xu, Hui (Miss)	CATT	3GPPMEMBER (ETSI)	CN
Xu, Lydia (Ms.)	Huawei Technologies Sweden AB	3GPPMEMBER (ETSI)	CN
Zhang, Dajiang (Mr.)	Nokia Japan Co, Ltd	3GPPMEMBER (ARIB)	JP
Zhang, Dongmei (Miss)	Huawei Technologies Japan Co.,	3GPPMEMBER (ARIB)	JP
Zhang, Emma (Miss)	HiSilicon Technologies Co., Lt	3GPPMEMBER (CCSA)	GB
Zhang, Mengwang (Mr.)	ZTE Corporation	3GPPMEMBER (ETSI)	CN
Zhao, Ping (Mr.)	China Telecommunications	3GPPMEMBER (ETSI)	CN
Zhu, Judy (Miss)	China Mobile Com. Corporation	3GPPMEMBER (CCSA)	CN

Zhu, Li (Mr.)	ZTE Corporation	3GPPMEMBER (CCSA)	CN
Zugenmaier, Alf (Dr.)	NTT DOCOMO INC.	3GPPMEMBER (ARIB)	DE
Zumerle, Dionisio (Ing.)	ETSI	3GPPORG_REP (ETSI)	FR
Zuo, Min (Miss)	China Mobile Com. Corporation	3GPPMEMBER (CCSA)	CN

57 Delegates attending.

Annex I: List of future meetings

See clause 10.