|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Agenda** | **Topic** | **TDoc** | **Title** | **Source** | **Type** | **Notes** | **Decision** | **Replaced-by** |
| 1 | Agenda and Meeting Objectives | S3‑221310 | Agenda | SA WG3 Chair | agenda |  | available |  |
|  |  | S3‑221311 | Process for SA3#107e meeting | SA WG3 Chair | other |  | available |  |
|  |  | S3‑221312 | Process and agenda for SA3#107e | SA WG3 Chair | other | >>CC\_1<<  [Chair] presents current status  >>CC\_1<< | available |  |
| 2 | Meeting Reports |  |  |  |  |  |  |  |
| 3 | Reports and Liaisons from other Groups (related to studies in the agenda) | S3‑221315 | LS on user’s consent for EDGEAPP | C3-223780 | LS in | >>CC\_1<<  [Rapporteur] presents  [Huawei] there are two related LS reply, proposes to give reply to CT3 based on Huawei’s contribution.  >>CC\_1<< | available |  |
|  |  | S3‑221476 | [DRAFT] Reply LS on user’s consent for EDGEAPP | Ericsson | LS out | >>CC\_1<<  [Ericsson] presents  >>CC\_1<< | available |  |
|  |  | S3‑221420 | Reply LS on User Consent for EDGEAPP | Huawei, HiSilicon | LS out | >>CC\_1<<  [Huawei] presents, proposes to merge and take 1420 as baseline.  Discussion between [Huawei] and [Ericsson].  [Ericsson] volunteers to hold the pen.  >>CC\_1<< | available |  |
|  |  | S3‑221317 | LS on V2X PC5 link for unicast communication with null security algorithm | R5-222035 | LS in | >>CC\_1<<  [Huawei] presents, but with bad connection.  [Lenovo] presents. proposes to merge two draft proposals to reply.  [QC] points out there is CT1 reply, proposes to include CT1 LS into agenda and consider it also while replying to the LS.  Chair asks MCC to include CT1 LS. (assigned as S3-221587)  Chair asks to continue email discussion.  >>CC\_1<< | available |  |
|  |  | S3‑221405 | Reply LS about V2X PC5 unicast link with null security algorithm | Huawei, HiSilicon | LS out | >>CC\_1<<  Related with 1317  >>CC\_1<< | available |  |
|  |  | S3‑221535 | DRAFT Reply LS on V2X PC5 link for unicast communication with null security algorithm | Lenovo | LS out | >>CC\_1<<  Related with 1317  >>CC\_1<< | available |  |
|  |  | S3‑221584 | Null algorithm is not security deactivation | Lenovo | draftCR | >>CC\_1<<  Related with 1317  >>CC\_1<< | available |  |
|  |  | S3‑221393 | Reply LS on Clarification on MBS Security Keys | Huawei, HiSilicon | LS out | >>CC\_1<<  [Huawei] presents current status.  [Nokia] comments rewording is needed.  [QC] comments the answer is not correct.  [Samsung] comments from email.  [Huawei] is open to discuss via email.  Chair requests to keep email discussion.  >>CC\_1<< | available |  |
|  |  | S3‑221316 | LS to 3GPP CT4 on Identification of source PLMN-ID in SBA | GSMA | LS in |  | withdrawn |  |
|  |  | S3‑221536 | Null algorithm is not security deactivation | Lenovo | CR |  | withdrawn |  |
| 4 | Work areas (No normative work included in this meeting) |  |  |  |  |  |  |  |
| 5 | Studies areas |  |  |  |  |  |  |  |
| 5.1 | Study on 5G security enhancement against false base stations | S3‑221364 | Addressing the editor’s note in 6.27.2.1.1 of Sol#27 | CableLabs, Deutsche Telekom, Philips International B.V. | pCR |  | available |  |
|  |  | S3‑221366 | Addressing EN on NR Repeater in 6.27.2.2.4 of Sol#27 | CableLabs | pCR |  | available |  |
|  |  | S3‑221368 | Addressing the editor’s note in 6.27.2.2.1of Sol#27 | CableLabs, Deutsche Telekom, Philips International B.V. | pCR |  | available |  |
|  |  | S3‑221370 | LS out on authenticity and replay protection of system information | CableLabs, Deutsche Telekom, Philips International B.V., Ericsson, InterDigital, Apple, Johns Hopkins University APL, NIST | LS out | >>CC\_1<<  [CableLabs] presents.  [Nokia] is ok with contribution, but a question whether 64 bytes are only choice?  [CableLabs] replies 64bytes is just an example.  [Nokia] asks to revise to reduce possible misunderstanding.  [QC] doesn’t agree. There is no need to send LS to RAN.  [Apple] replies to QC. It helps. And supports to send LS  [Docomo] comments on question 1. It needs to figure out what is the length of signature, not just an example. And asks questions. Proposes to revise Q1.  [Huawei] is fine with proposal in general, but Q2 is not clear. Need to be clarified.  [Samsung] supports  [Intel] supports. Proposes to put reference to the TR solutions while referring to solutions in the LS.  [IDCC] supports, but be careful while asking RAN about quantum safe algo. It is SA3 job.  [Docomo] replies to IDCC. Wants to know the limit of length the length of key that can be accommodated, not on Quantum safe algorithms itself..  [CableLabs] replies, agrees to reformulate the questions  [QC] comments, when solutions are not agreed or not feasible what is the point in asking the questions to RAN2..  Chair request to continue email discussion.  >>CC\_1<< | available |  |
|  |  | S3‑221371 | Evaluation of solution #4 | Huawei, HiSilicon, Ericsson, Apple, Philips | pCR | >>CC\_1<<  [Huawei] presents the content and current status  [QC] comments the status is not correct.  [Apple] comments the current content comes from RAN, if there is more evaluation, it could bring contribution to add.  [QC] request to keep EN.  [Docomo] questions about other Tdoc# and WG names in evaluation part.  MCC suggest to revise the text.  [Huawei] replies.  [QC] comments to let Huawei prepare a revision to implement comments and then add their comment.  >>CC\_1<< | available |  |
|  |  | S3‑221464 | 5GFBS - Security risk in lower layers | Apple | pCR | [Nokia]: Agree with minor re-wording. | available |  |
|  |  | S3‑221572 | Detection of MitM attacks with secret paging | Lenovo | pCR | [Nokia]: Do not agree and ask for clarification. | available |  |
| 5.2 | Study on Security Impacts of Virtualisation | S3‑221318 | Solution 5 EN on Certificates and Tokens | U.S. National Security Agency | pCR | [Ericsson]: proposes to capture relevant part of the rationale in the evaluation  >>CC\_1<<  [US NSA] will revise with comments tomorrow.  [Docomo] It is weird about 1st EN.  [US NSA] clarifies.  [Nokia] comments.  [Huawei] comments to have some evaluation before simply removal of EN.  >>CC\_1<< | available |  |
|  |  | S3‑221337 | Updates to Solution #5 | Johns Hopkins University APL, US National Security Agency, CableLabs, InterDigital, AT&T, CISA ECD | pCR | [Ericsson]: Changes proposed -r1 {https://www.3gpp.org/ftp/tsg\_sa/WG3\_Security/TSGS3\_107e-AdHoc/Inbox/Drafts/draft\_S3-221377-r1\_Updates\_to\_Solution5.doc} .  >>CC\_1<<  [JHU] presents  [Ericsson] r1 is uploaded and asks to check.  [Huawei] comments with bad connection.  Chair request to continue discussion over email.  >>CC\_1<< | available |  |
|  |  | S3‑221338 | Address EN on Run-time Attestation | Johns Hopkins University APL, US National Security Agency, CableLabs, InterDigital, AT&T, CISA ECD | pCR | >>CC\_1<<  [JHU] presents.  [Huawei] proposes to move run-time attestation related wording from evaluation.  [Docomo] comments run-time wording is not clear.  [JHU] clarifies.  >>CC\_1<< | available |  |
|  |  | S3‑221339 | Remove EN in clause 6.6.3.4 | Johns Hopkins University APL, US National Security Agency, CableLabs, InterDigital, AT&T, CISA ECD | pCR | >>CC\_1<<  [JHU] presents  Chair requests to continue email discussion  >>CC\_1<< | available |  |
|  |  | S3‑221392 | Update of KI #3 to contribute an EN | Huawei, HiSilicon | pCR | >>CC\_1<<  [Huawei] presents.  Chair requests to continue email discussion  >>CC\_1<< | available |  |
|  |  | S3‑221404 | evaluation on solution 5 | Huawei, HiSilicon | pCR | >>CC\_1<<  [Huawei] presents  [JHU] comments 1337 can address some evaluation made in this contribution.  >>CC\_1<< | available |  |
|  |  | S3‑221485 | New solution on boot time attestation at 3GPP function level | Huawei, HiSilicon | pCR | >>CC\_1<<  [Huawei] presents  [JHU] concerns. Some ENs are needed.  [Thales] comments. Clarification is needed and proposes to note this one.  Chair asks to continue discussion.  >>CC\_1<< | available |  |
|  |  | S3‑221486 | New solution on trust domain and slice Isolation | Huawei, HiSilicon | pCR | >>CC\_1<<  [Huawei] presents.  Chair asks to continue discussion.  >>CC\_1<< | available |  |
| 5.3 | Study on Security Aspects of Proximity Based Services in 5GS Phase 2 | S3‑221330 | Key issue on Privacy protection over the UE-to-UE Relay | InterDigital, Europe, Ltd. | pCR |  | available |  |
|  |  | S3‑221331 | Key Issue on Authorization in the UE-to-UE Relay Scenario | InterDigital, Europe, Ltd. | pCR |  | available |  |
|  |  | S3‑221332 | Key Issue on Security of UE-to-UE Relay | InterDigital, Europe, Ltd. | pCR |  | available |  |
|  |  | S3‑221383 | Integrity and confidentiality of information over the UE-to-UE Relay | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221406 | New Key Issue on security of ProSe groupcast communications | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221418 | Authorization in the UE-to-UE relay scenario | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221419 | Privacy of information over the UE-to-UE Relay | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221421 | Key issue on Authorization in the UE-to-UE relay scenario | China Telecomunication Corp. | pCR |  | available |  |
|  |  | S3‑221422 | Key issue on Integrity and confidentiality of information over the UE-to-UE | China Telecomunication Corp. | pCR |  | available |  |
|  |  | S3‑221423 | Key issue on Secondary authentication of Remote UE via L3 UE-to-Network relay without N3IWF | China Telecomunication Corp. | pCR |  | available |  |
|  |  | S3‑221426 | Key issue on authorization in multi-path transmission for UE-to-Network Relay scenario | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221427 | Key issue on authorization in the UE-to-UE relay scenario | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221428 | Key issue on Integrity and confidentiality of information over the UE-to-UE Relay | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221429 | Key issue on Privacy of information over the UE-to-UE Relay | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221430 | Key issue on Support direct communication path switching between PC5 and Uu | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221446 | Key issue on UE Identity protection during UE-to-UE relay discovery | China Telecomunication Corp. | pCR |  | available |  |
|  |  | S3‑221447 | Key issue on Privacy protection over the UE-to-UE Relay | China Telecomunication Corp. | pCR |  | available |  |
|  |  | S3‑221491 | pCR to TR33.740 Key Issue on Integrity and confidentiality of information over the UE-to-UE Relay | CATT | pCR |  | available |  |
|  |  | S3‑221495 | pCR to TR33.740 Key Issue on Authorization in the UE-to-UE relay scenario | CATT | pCR |  | available |  |
|  |  | S3‑221496 | pCR to TR33.740 Key Issue on Privacy of information over the UE-to-UE Relay | CATT | pCR |  | available |  |
|  |  | S3‑221503 | Remote UE Security Establishment via U2U Relay | OPPO | pCR |  | available |  |
|  |  | S3‑221505 | U2U Relay Trust Model | OPPO | pCR |  | available |  |
|  |  | S3‑221519 | New Key Issue: Security for UE-to-UE Relay discovery | Qualcomm Incorporated | pCR |  | available |  |
|  |  | S3‑221548 | Key Issue on Security for UE-to-UE Relay Discovery | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221549 | Key Issue on Security of UE-to-UE Relay Communication | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221425 | Add context to the architecture clause | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221489 | pCR to TR33.740 Clause Introduction and Scope | CATT | pCR |  | available |  |
|  |  | S3‑221490 | pCR to TR 33.740 Clause 4 Security Aspects of 5G ProSe | CATT | pCR |  | available |  |
| 5.4 | Study on privacy of identifiers over radio access | S3‑221340 | New key issue on users identified by Priority Access | Johns Hopkins University APL, US National Security Agency, CISA ECD, Peraton Labs, Interdigital, Apple | pCR |  | available |  |
|  |  | S3‑221517 | Scope of SUPI Type IMSI in KI#1 | Qualcomm Incorporated | pCR |  | available |  |
|  |  | S3‑221518 | Addition of threats due to EAP in KI#1 | Qualcomm Incorporated | pCR |  | available |  |
|  |  | S3‑221460 | Padding-based solution to the leakage of the length of SUPI through SUCI. | Ericsson LM | pCR |  | available |  |
|  |  | S3‑221462 | Hash-based solution to the leakage of the length of SUPI through SUCI | Ericsson LM | pCR |  | available |  |
|  |  | S3‑221463 | Map-based solution to the leakage of the length of SUPI through SUCI | Ericsson LM | pCR |  | available |  |
|  |  | S3‑221329 | New solution for Key issue #1 | InterDigital, Inc. | pCR |  | available |  |
|  |  | S3‑221431 | SUPI padding solution on Key issue #1 | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221378 | Solution for Privacy aspects of variable length user identifiers | Nokia Japan | pCR |  | available |  |
|  |  | S3‑221410 | New solution for key issue 1 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221465 | IDPrvc - Security issue on C-RNTI | Apple | pCR |  | available |  |
| 5.5 | Study on Standardising Automated Certificate Management in SBA | S3‑221585 | Key Issue for Management of Automated Bulk Certificate updates for SBA leading to temporary service unavailability | Nokia Japan | pCR |  | available |  |
|  |  | S3‑221381 | Update KI #6 for a new security threat | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221382 | New solution for KI #6 Relation between certificate management lifecycle and NF management lifecycle | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221473 | A solution for certificate and NF lifecycle management relation | Ericsson | pCR |  | available |  |
|  |  | S3‑221408 | New solution for key issue 1 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221475 | A new solution of using CMP for certificate enrolment and renewal | Ericsson | pCR |  | available |  |
|  |  | S3‑221409 | New solution for key issue 3 and 4 based on OCSP | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221474 | A new solution for using attestation to build initial trust for certificate management | Ericsson | pCR | [Deutsche Telekom] : asks further clarification of the Note | available |  |
|  |  | S3‑221501 | Solution for secure initial enrolment of NF certificates | Nokia, Nokia Shanghai Bell | pCR | [Deutsche Telekom] : Supports the new enrolment solution proposal | available |  |
|  |  | S3‑221552 | New solution on Cross-Certification Based Trust Chain in the SBA Architecture | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221553 | New solution on Interconnection CA Based Trust Chain in the SBA Architecture | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221380 | Key Issue for Management of Automated Bulk Certificate updates for SBA leading to temporary service unavailability | Nokia Japan | pCR |  | revised | [S3‑221585](file:///C:\Users\cmcc\Desktop\AgendaWithTdocAllocation_2022-06-24_15h19.htm#RANGE!S3-221585) |
| 5.6 | New SID on AKMA phase 2 | S3‑221351 | Update in KI1 for encryption keys | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221356 | Key Issue for AKMA roaming scenario | THALES | pCR |  | available |  |
|  |  | S3‑221435 | Update the Key issue of AKMA roaming | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221529 | Adding security threat and requirements to KI#1 | Samsung | pCR |  | available |  |
|  |  | S3‑221457 | New key issue of multiple AAnF sets in AKMA roaming scenario | LG Electronics France | pCR |  | available |  |
|  |  | S3‑221558 | New KI Multiple registrations in AKMA scenarios | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221352 | Solution on AKMA roaming | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221384 | new solution for AKMA roaming when both UE and AF are in VPLMN | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221385 | new solution for AKMA roaming when UE is in visited network but the AF in Home network. | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221433 | New solution about the roaming AKMA architecture of the AF inside and outside the HPLMN | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221434 | New solution about the roaming AKMA architecture of the AF inside and outside the VPLMN | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221459 | New solution of AKMA anchor key registration to the AAnF in VPLMN after primary authentication | LG Electronics France | pCR |  | available |  |
|  |  | S3‑221554 | KI#1, New Sol AKMA Application key request via proxy and NEF in roaming scenarios | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221555 | KI#1, New Sol Proxy-based AKMA Application key request in roaming scenarios | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221571 | AKMA roaming and LI | Lenovo | pCR |  | available |  |
|  |  | S3‑221432 | Discussion on the regulatory control point in AKMA roaming | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221456 | Discussion paper of AKMA roaming | China Mobile | discussion |  | available |  |
|  |  | S3‑221581 | Discussion about the roaming architecture | Ericsson | discussion |  | available |  |
|  |  | S3‑221458 | Solution of introducing AP into AKMA | China Mobile | pCR |  | available |  |
|  |  | S3‑221466 | AKMA - New solution on AP | Apple | pCR |  | available |  |
|  |  | S3‑221516 | AKMA Application Proxy solution based on GBA procedures | Qualcomm Incorporated | pCR |  | available |  |
|  |  | S3‑221556 | KI#2, New Sol Authentication via proxy AKMA scenarios. | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221557 | KI#2, New Sol Authentication via proxy and NEF in AKMA scenarios | Xiaomi Communication | pCR |  | available |  |
| 5.7 | Study of Security aspect of home network triggered primary authentication | S3‑221386 | Skeleton update | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221387 | new KI in interworking | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221388 | new KI in SoR/UPU counter wraparound | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221389 | new KI in Kakma refresh | Huawei, HiSilicon | pCR | [Nokia]: Ask clarification and propose changes. | available |  |
|  |  | S3‑221524 | Corrections to TR 33.741 | Lenovo | pCR |  | available |  |
|  |  | S3‑221391 | New KI on race condition | Huawei, HiSilicon | pCR | [Nokia]: Ask for clarification. | available |  |
|  |  | S3‑221580 | KI#2 update to remove the signalling overhead for KAF | Ericsson | pCR |  | available |  |
|  |  | S3‑221390 | AUSF triggered the primary authentication | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221525 | Solution to enable HN triggered Primary Authentication with AUSF | Lenovo | pCR |  | available |  |
|  |  | S3‑221526 | Solution to enable HN triggered Primary Authentication with UDM | Lenovo | pCR |  | available |  |
|  |  | S3‑221530 | New solution on HN initiated re-authentcation via AUSF | Samsung | pCR |  | available |  |
|  |  | S3‑221551 | New solution on AUSF initiated Primary Authentication | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221353 | Solution on HN triggering primary authentication for various scenarios | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221415 | New solution UDM triggered primary authentication | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221436 | Home network triggered authentication solution for 4G to 5G interworking on Key issue #1 | ZTE Corporation | pCR | [Nokia]: Ask for clarification. | available |  |
|  |  | S3‑221498 | New solution on KI#1 AMF based solution | NEC Corporation | pCR | [Nokia]: Ask for clarification | available |  |
|  |  | S3‑221515 | Solution using UDM to trigger authentication | Qualcomm Incorporated | pCR |  | available |  |
|  |  | S3‑221531 | New solution on UDM initiated re-authentcation based on AUSF request | Samsung | pCR |  | available |  |
|  |  | S3‑221532 | New solution for Kaf refresh | Samsung | pCR |  | available |  |
|  |  | S3‑221550 | New solution on UDM initiated Primary Authentication | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221354 | Solution on Kaf refresh without primary authentication -UA\* | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221355 | Solution on Kaf refresh without primary authentication- AAnF | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221437 | Kaf update solution without triggering primary authentication on Key issue #2 | ZTE Corporation | pCR | [LGE] : Asks for clarification on K\_AUSF regeneration.  [Nokia]: Ask for clarification | available |  |
|  |  | S3‑221472 | New solution Security procedure of KAF refresh-MAC | OPPO | pCR | [Nokia]: Ask for clarification | available |  |
|  |  | S3‑221480 | New solution Security procedure of KAF refresh-Counter | OPPO | pCR | [Nokia]: Ask for clarification | available |  |
|  |  | S3‑221481 | New solution Security procedure of KAF-Nonce | OPPO | pCR |  | available |  |
|  |  | S3‑221497 | New solution on KI#1 UE based solution | NEC Corporation | pCR | [Nokia]: Ask for clarification | available |  |
|  |  | S3‑221576 | Discussion about the home triggered primary authentication for interworking | Ericsson | discussion |  | available |  |
|  |  | S3‑221577 | Conclusion for the primary authentication upon interworking from EPS to 5GS | Ericsson | pCR |  | available |  |
|  |  | S3‑221578 | Discussion about the need for initiating home triggered primary authentication for the SoR/UPU use case. | Ericsson | discussion |  | available |  |
|  |  | S3‑221579 | Conclusion for the primary authentication upon SoR and UPU counter wrap around. | Ericsson | pCR |  | available |  |
| 5.8 | Study on security aspects of enablers for Network Automation for 5G - phase 3 | S3‑221451 | Anomaly in Multivendor NWDAF Framework | Intel | pCR |  | available |  |
|  |  | S3‑221453 | Revision on KI#2 | China Mobile Com. Corporation | pCR |  | available |  |
|  |  | S3‑221454 | KI on Security for NWDAF-assisted application detection | China Mobile Com. Corporation | pCR |  | available |  |
|  |  | S3‑221533 | Key issue on Cyber-attack detection supported by NWDAF | Samsung | pCR |  | available |  |
|  |  | S3‑221365 | New solution on authorization of AI/ML model retrieving | China Telecommunications | pCR |  | available |  |
|  |  | S3‑221452 | Authorization and Authentication of ML model transfer | Intel | pCR |  | available |  |
|  |  | S3‑221470 | Solution for AI-ML model authorization and retrieval | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221570 | AI/ML model storage and sharing security | Lenovo | pCR |  | available |  |
|  |  | S3‑221367 | New solution on Using Federated-Learning-related Analytics Id for authorization of selection of participant NWDAF instances in the Federated Learning group | China Telecommunications | pCR |  | available |  |
|  |  | S3‑221369 | New solution on topology hiding in data and analytics exchange in roaming case | China Telecommunications | pCR |  | available |  |
|  |  | S3‑221471 | Solution for access control and anonymization for data and analytics exchange in roaming | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221469 | Solution for anomalous NF behaviour detection by NWDAF | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
| 5.9 | Study on Security Enhancement of support for Edge Computing — phase 2 | S3‑221320 | New key issue on UE privacy protection and authorization in NW exposure of UE traffic related information to AF | InterDigital Communications | pCR |  | available |  |
|  |  | S3‑221322 | New key issue on Authorization for ACR | InterDigital Communications | pCR |  | available |  |
|  |  | S3‑221323 | New key issue on ACR security | InterDigital Communications | pCR |  | available |  |
|  |  | S3‑221411 | New KI on Authentication and Authorization between V-ECS and H-ECS | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221412 | New KI on Transport security for the EDGE10 interface | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221413 | New KI on Authentication and Authorization between AC and EEC | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221477 | Updates to authentication and authorization key issue | Ericsson | pCR |  | available |  |
|  |  | S3‑221487 | New KI on data protection for the fast and efficient network exposure | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221488 | New KI on how to authorize PDU session to support local traffic routing to access an EHE in the VPLMN | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221357 | Solution for Key Issue #2.2 | THALES | pCR |  | available |  |
|  |  | S3‑221377 | New solution Authentication mechanism selection in EDGE | OPPO | pCR |  | available |  |
|  |  | S3‑221379 | New solution Authentication mechanism selection among EEC, ECS, and EES | OPPO | pCR |  | available |  |
|  |  | S3‑221399 | Authentication mechanism selection between the EEC and ECS/EES | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221438 | ECS EES authentication method information provisioning solution on Key issue #2.2 | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221467 | MEC - Negotiation procedure for the authentication and authorization | Apple | LS out |  | available |  |
|  |  | S3‑221527 | Authentication mechanism selection between EEC and ECS | Samsung | pCR |  | available |  |
|  |  | S3‑221528 | Authentication mechanism selection between EEC and EES | Samsung | pCR |  | available |  |
|  |  | S3‑221559 | KI#2.1, New Sol Authentication and authorization between EEC hosted in the roaming UE and ECS | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221560 | KI#2.1, New Sol Authentication and authorization between EEC hosted in the roaming UE and EES | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221561 | KI#2.2, New Sol 5GC-based authentication mechanism selection between EEC and ECS or EES | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221468 | HN-auth-NAS based HN triggered authentication | Apple | pCR |  | available |  |
| 5.10 | Study on Personal IoT Networks Security Aspects | S3‑221319 | New key issue on Protecting Identification of PIN and PIN Privacy | InterDigital, Inc. | pCR |  | available |  |
|  |  | S3‑221321 | New key issue on Secure Communication of between PINEs | InterDigital, Inc. | pCR | [Nokia]: Requires major clarification and update. | available |  |
|  |  | S3‑221325 | New key issue on Secure policy and parameters provisioning for PIN | InterDigital, Inc. | pCR | [Nokia]: Requests update | available |  |
|  |  | S3‑221327 | New key issue on Authorization of PINE | InterDigital, Inc. | pCR |  | available |  |
|  |  | S3‑221328 | New key issue on PIN and PINE discovery authorization | InterDigital, Inc. | pCR | [Nokia]: Proposes to postpone. | available |  |
|  |  | S3‑221335 | New Key Issue on controlling access of PIN elements to 5G network | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221417 | Authentication and authorization to PINE behind PEGC and PEMC | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221440 | Key issue on secure data transfer between PEGC PEMC and PIN NF | ZTE Corporation | pCR | [Nokia]: Proposes to postpone or note. | available |  |
|  |  | S3‑221502 | Proposed skeleton for TR 33.882 | vivo Mobile Communication (S) | pCR |  | available |  |
|  |  | S3‑221504 | Scope of TR 33.882 | vivo Mobile Communication (S) | pCR |  | available |  |
|  |  | S3‑221506 | New KI for authentication of PINE | vivo Mobile Communication (S) | pCR |  | available |  |
|  |  | S3‑221507 | New Key Issue for controlling of remote provisioning | vivo Mobile Communication (S) | pCR |  | available |  |
|  |  | S3‑221564 | New KI: Secure authentication of PINE | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221565 | New KI: Secure provisioning of credentials for non-3GPP device via PEGC | Xiaomi Communication | pCR |  | available |  |
| 5.11 | Study on SNAAPP security | S3‑221314 | skeleton for draft TR 33.884 SNAAPP security(FS\_SNAAPPY) | NTT DOCOMO | draft TR |  | available |  |
|  |  | S3‑221336 | New Key Issue on Securing API invocation from UE applications | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221359 | pCR to 33.884, scope | NTT DOCOMO | pCR |  | available |  |
|  |  | S3‑221478 | A new key issue on authentication and authorization of UE in UE originated API invocation | Ericsson | pCR |  | available |  |
|  |  | S3‑221479 | A new key issue on user consent in API invocations | Ericsson | pCR |  | available |  |
|  |  | S3‑221582 | pCR to 33.884, key issues from scope objective 1 | NTT DOCOMO | pCR |  | withdrawn |  |
|  |  | S3‑221586 | LS on CAPIF authorization roles related to FS\_SNAAPP | S6-221771 | LS in | >>CC\_1<<  [Docomo] presents and proposes way forward  [Huawei] agrees with Docomo observation.  [CableLabs] asks questions to Docomo and Huawei.  [Apple] asks whether there is a draft reply.  [Docomo] replies there is not yet.  Chair asks to continue email discussion and asks Docomo to hold the pen if there is progress and response.  >>CC\_1<< | available |  |
| 5.12 | Study on enhanced security for network slicing Phase 3 | S3‑221372 | Skeleton of TR33.886 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221373 | Scope of TR33.886 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221374 | New KI-providing VPLMN slice information to roaming UE | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221375 | New KI-temprory slices and slice authorization | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221376 | New KI on NSAC | Huawei, HiSilicon | pCR |  | available |  |
| 5.13 | Study on Security aspects for 5WWC Phase 2 | S3‑221341 | Skeleton for 5WWC Ph2 study | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221342 | Scope of 5WWC study | Nokia, Nokia Shanghai Bell, CableLabs | pCR |  | available |  |
|  |  | S3‑221343 | Key issue on authentication of AUN3 device not supporting EAP | Nokia, Nokia Shanghai Bell, CableLabs | pCR |  | available |  |
|  |  | S3‑221344 | Key issue on authentication of AUN3 device supporting EAP | Nokia, Nokia Shanghai Bell, CableLabs | pCR |  | available |  |
|  |  | S3‑221345 | Key issue on Authentication of UE behind RG and connected via NSWO | Nokia, Nokia Shanghai Bell, CableLabs | pCR |  | available |  |
|  |  | S3‑221346 | Key issue on Security aspect of slice information exposure of N3IWF/TNGF | Nokia, Nokia Shanghai Bell, CableLabs | pCR |  | available |  |
|  |  | S3‑221416 | authentication and authorization to N3GPP device behind 5G-RG | Huawei, HiSilicon | pCR |  | available |  |
| 5.14 | Study on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NG-RAN | S3‑221573 | TR skeleton | Ericsson | draft TR |  | available |  |
|  |  | S3‑221574 | Content for the scope clause of the technical report | Ericsson | pCR |  | available |  |
|  |  | S3‑221575 | Initial content for the background clause of the technical report | Ericsson | pCR |  | available |  |
| 5.15 | Study on security support for Next Generation Real Time Communication services | S3‑221482 | skeleton for NGRTC | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221483 | Scope of TR 33.890 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221484 | New KI on 3rd party ID | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221546 | Key Issue on Authorization for Third Party Specific User ID Usage | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221547 | Key Issue on Verification of the Third Party User Specific ID | Beijing Xiaomi Mobile Software | pCR |  | available |  |
| 5.16 | Study on security aspects of enhanced support of Non-Public Networks phase 2 | S3‑221361 | Key issue on connected and idle mode mobility | Nokia, Nokia Shanghai Bell | pCR | [Ericsson]: proposal to note | available |  |
|  |  | S3‑221362 | Key issue on non-3GPP access in SNPN’s | Nokia, Nokia Shanghai Bell | pCR | [Ericsson]: proposes to merge in S3-221493  [Nokia]: Accepts proposal to merge and clarifies. | available |  |
|  |  | S3‑221363 | Key issue on providing access to localised services | Nokia, Nokia Shanghai Bell | pCR | [Ericsson]: proposes to merge in S3-221494  [Nokia]: Accepts proposal to merge and provides clarifications. | available |  |
|  |  | S3‑221450 | Authentication and Authorization for Localized Services | Intel | other | [Ericsson]: proposes to merge in S3-221494 | available |  |
|  |  | S3‑221492 | Scope for Study on security aspects of enhanced support of Non-Public Networks phase 2 | Ericsson | pCR |  | available |  |
|  |  | S3‑221493 | New Key Issue "Security of non-3GPP access for SNPN" | Ericsson | pCR |  | available |  |
|  |  | S3‑221494 | New Key Issue "Hosting network and UE mutual authentication" | Ericsson | pCR |  | available |  |
|  |  | S3‑221562 | New KI: Home control enhancement for eNPN | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221563 | New KI: Support for secure non-3GPP access for NPN | Xiaomi Communication | pCR | [Ericsson]: proposes to merge in S3-221493  [Xiaomi]: is ok with the merge suggestion. | available |  |
| 5.17 | Study on Security of Phase 2 for UAS, UAV and UAM | S3‑221333 | Key Issue on Direct C2 Security | InterDigital, Europe, Ltd. | pCR |  | available |  |
|  |  | S3‑221334 | Key Issue on Direct C2 Authorization | InterDigital, Europe, Ltd. | pCR |  | available |  |
|  |  | S3‑221407 | New Key Issue on security enhancement of C2 communication | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221514 | Key issue for security of unicast connection | Qualcomm Incorporated | other |  | available |  |
|  |  | S3‑221512 | Proposed skeleton for TR 33.891 | Qualcomm Incorporated | other |  | available |  |
|  |  | S3‑221513 | Proposed scope for TR 33.891 | Qualcomm Incorporated | other |  | available |  |
|  |  | S3‑221534 | Key issue on Privacy and security aspects of broadcasting Remote ID | Samsung | pCR |  | available |  |
| 5.18 | Study to enable URSP rules to securely identify Applications | S3‑221567 | Skeleton for TR 33.892 FS\_USIA | Lenovo | draft TR |  | available |  |
|  |  | S3‑221568 | Scope for TR 33.892 | Lenovo | pCR | [Nokia]: Request clarifications to the scope before acceptable.  MCC commented on the scope. | available |  |
|  |  | S3‑221569 | KI on determination of additional information for application identification | Lenovo | pCR |  | available |  |
| 5.19 | Study on Security Aspects of Ranging Based Services and Sidelink Positioning | S3‑221537 | 33.893: Draft Skeleton | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221538 | 33.893: Scope | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221441 | Add context to the architecture assumption | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221539 | 33.893: Architecure Assumptions | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221398 | New key issue on privacy protection for Ranging/Sidelink positioning with the assistance of assistant UE | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221455 | Key issue on Privacy protection for Network assisted Sidelink Positioning | China Telecomunication Corp. | pCR |  | available |  |
|  |  | S3‑221540 | 33.893: New Key Issue on Privacy | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221442 | Key issue on discovery message protection between reference UEs and target UEs | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221542 | 33.893: New Key Issue on Discovery Security | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221443 | Key issue on security of network based sidelink positioning | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221445 | Key issue on security of UE based sidelink positioning | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221543 | 33.893: New Key Issue on Direct Communication Security | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221444 | Key issue on security of service exposure to a UE | ZTE Corporation | pCR |  | available |  |
|  |  | S3‑221541 | 33.893: New Key Issue on Authorization for Ranging/SL Positioning Service | Beijing Xiaomi Mobile Software | pCR |  | available |  |
|  |  | S3‑221360 | Key issue on application impersonation | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
| 5.20 | Study on Security and Privacy of AI/ML-based Services and Applications in 5G | S3‑221313 | LS on 5GC information exposure to UE | S2-2205286 | LS in |  | available |  |
|  |  | S3‑221358 | draft-LS reply on 5GC information exposure to UE | NTT DOCOMO | LS out |  | available |  |
|  |  | S3‑221511 | Draft LS on 5GC Information Exposure to UE | OPPO | LS out |  | available |  |
|  |  | S3‑221583 | TR 33.898 Skeleton | OPPO | pCR |  | available |  |
|  |  | S3‑221509 | Scope of TR 33.898 | OPPO | pCR |  | available |  |
|  |  | S3‑221510 | References in TR 33.898 | OPPO | pCR |  | available |  |
|  |  | S3‑221347 | Key issue on authorization of AIML operations | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221349 | Key issue on securing AIML operation | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221324 | New key issue on Federated Learning AIML model protection | InterDigital Communications | pCR |  | available |  |
|  |  | S3‑221350 | Key issue on Security criteria of UE selection for AIML | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221326 | New key issue on Federated Learning AIML model privacy protection | InterDigital Communications | pCR |  | available |  |
|  |  | S3‑221566 | New KI: Privacy-preserving federated learning | Xiaomi Communication | pCR |  | available |  |
|  |  | S3‑221348 | Key issue on authorization of UE accessing the 5G analytics | Nokia, Nokia Shanghai Bell | pCR |  | available |  |
|  |  | S3‑221508 | TR 33.898 Skeleton | OPPO | pCR |  | revised | [S3‑221583](file:///C:\Users\cmcc\Desktop\AgendaWithTdocAllocation_2022-06-24_15h19.htm#RANGE!S3-221583) |
| 5.21 | Study on applicability of the Zero Trust Security principles in mobile networks | S3‑221520 | Proposal for TR 33.894 Skeleton | Lenovo | other |  | available |  |
|  |  | S3‑221523 | Update of Scope | Lenovo, Rakuten Mobile Inc, Interdigital, US NSA, Motorola Solutions, Johns Hopkins University APL, Intel, Center for Internet Security | pCR |  | available |  |
|  |  | S3‑221522 | Security Assumptions | Lenovo, Rakuten Mobile Inc., Interdigital, US NSA, Motorola Solutions, Johns Hopkins University APL, Intel, Center for Internet Security | pCR |  | available |  |
|  |  | S3‑221439 | new key issue Exposure of Network Capabilities | ZTE Corporation | pCR | [Lenovo]: Propose to merge S3-221439 in S3-221521.  [CMCC] proposes to revise | available |  |
|  |  | S3‑221449 | Key Issue on Secure Trust Evaluation | Intel | other | [Lenovo]: Propose to merge S3-221449 in S3-221521.  [CMCC] proposes to note | available |  |
|  |  | S3‑221500 | Key issue on determining and maintaining trust indication in 5G Core | Nokia, Nokia Shanghai Bell | pCR | [CMCC] does not agree  [Lenovo]: Propose to merge S3-221500 in S3-221521.  [Nokia]: provides clarifications  [CMCC] is not convinced and provides further comments.  NCSC supports contribution, disagrees with CMCC.  [CMCC] proposes to note. | available |  |
|  |  | S3‑221521 | Key Issue#1 on Need for continuous Trust evaluation | Lenovo, Nokia, Nokia Shanghai Bell, Rakuten Mobile Inc., Interdigital, US NSA, Motorola Solutions, Johns Hopkins University APL, Intel, Center for Internet Security | pCR | [Lenovo]: revision r1 uploaded.  [CMCC] supports and asks to co-sign. | available |  |
|  |  | S3‑221499 | Key issue on misuse of OAuth 2.0 access token by anomalous Network functions | Nokia, Nokia Shanghai Bell | pCR | [CMCC] proposes to revise before approval.  [Nokia]: request for clarification to proceed with the revision  [CMCC] is fine with revision proposal. | available |  |
|  |  | S3‑221448 | Key Issue on secure storage and limited access to NF credentials | Intel | other | [CMCC] does not agree. It is out of 3GPP scope. | available |  |
| 5.22 | Study of Security aspects on User Consent for 3GPP Services Phase 2 | S3‑221400 | Skeleton of UC3S\_Ph2 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221401 | Scope of UC3S\_Ph2 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221402 | New key issue on Roaming of eNA | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221403 | New Key Issue on NTN | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221424 | Key Issue for NTN specific user consent for UE location sharing | Nokia Japan | pCR |  | available |  |
|  |  | S3‑221544 | 33.896: New Key Issue on NTN Specific User Consent | Xiaomi Technology | pCR |  | available |  |
|  |  | S3‑221545 | 33.896: New Solution for NTN Specific User Consent | Xiaomi Technology | pCR |  | available |  |
| 5.23 | Study on security enhancements for 5G multicast-broadcast services Phase 2 | S3‑221394 | Skeleton of MBS phase2 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221395 | Scope of MBS phase2 | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221396 | New key issue on TMGI protection | Huawei, HiSilicon | pCR | [Ericsson]: Ask for clarification. | available |  |
|  |  | S3‑221397 | New key issue on security handling in MOCN network sharing scenario | Huawei, HiSilicon | pCR | [Ericsson]: Changes proposed -r1 {https://www.3gpp.org/ftp/tsg\_sa/WG3\_Security/TSGS3\_107e-AdHoc/Inbox/Drafts/draft\_S3-221397-r1\_key%20issue%20on%20security%20handling%20in%20MOCN.docx} . | available |  |
|  |  | S3‑221414 | New key issue on security protection for Ues in RRC inactive state | Huawei, HiSilicon | pCR |  | available |  |
|  |  | S3‑221461 | Discussion paper about the security enhancements enabling UE’s receiving Multicast MBS Session data in RRC\_INACTIVE state | Ericsson | discussion |  | available |  |
| 6 | Any Other Business |  |  |  |  |  |  |  |