|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Agenda** | **Topic** | **TDoc** | **Title** | **Source** | **Type** | **Notes** | **Decision** | **Replaced-by** |
| 1 | Agenda and Meeting Objectives | S3‑240000 | Agenda | SA WG3 Chair | agenda |  | agreed |  |
|  |  | S3‑240001 | Detailed agenda | SA WG3 Chair | agenda |  | noted |  |
|  |  | S3‑240002 | Emeeting process | SA WG3 | agenda | <CC1>  Chair: official Monday, informal Tuesday, Wednesday, wind up official calls Thursday, Friday  E//: good proposal, Official Monday, Tuesday informal on Wednesday  E//: necessary to make comment known on email, too?  Chair: take official position on Thursday and Friday  Alf: taking notes, if they are incorrect, please send on email reflector the correct position.  QC: not ok for Friday meeting to have decision power  Chair: only for resolving contention  QC: 002 last revision should be 25 of jan, inconsistent with slide.  Chair: correct  QC: meeting with decision power  Chair: yes  Agenda agreed  </CC1>  <end of CC1>  Chair: Noamen please send list of GSMA related tdocs and maintenance  Noamen: ok  Huawei: some revisions are major rewrites, but not well justified  Nokia: some GSMA comments require major clarification  Mitre: GSMA comments should not limit us in case we see other instances of the same.  Huawei: some udates are missing references and justification  Chair: please provide concrete suggestions on email  E//: ask for correct work item to be used  Mirko: find WI code based on release  Huawei: for GSMA updates, we are targtting R18, use that work item  E//: so SCAS\_Ph3?  Huawei: yes, as it includes maintenance  </end of CC1  <CC3>  Huawei: concerns how to feedback to GSMA if there is no agreement on their proposals, as there will be a lot of work  GSMA: source of those comments come from regulators, if choose not to fix comments, the SCAS would not to be fit for purpose, so alternative could be common criteria  Chair: where would reconciliation take place?  GSMA: send LS to GSMA to explain why SA3 didn't fix some of the issues, and discuss with GSMA. Case by case.  Tmobile: GSMA looks at SCASes, mostly the comments are editorial, for GSMA to endorse new SCAS there will be a rigorous process.  Huawei: not in anyone's interest not to address the feedback, prefer to have an official LS from GSMA to which to respond,better to formalize the process a bit more  </CC3> | noted |  |
| 2 | Meeting Reports |  |  |  |  |  |  |  |
| 3 | Reports and Liaisons from other Groups ( related to SCAS) |  |  |  |  |  |  |  |
| 4 | Work areas |  |  |  |  |  |  |  |
| 4.1 | Maintenance(Rel-15/16/17/18) |  |  |  |  |  |  |  |
| 4.1.1 | Security Assurance | S3‑240003 | GSMA clarification: on unused software | BSI(DE) | CR | [Huawei] : request revision.  [BSI] : will provide revision.  <CC1>  Michael presents  Comments already on email  Mitre: editorials  </CC1>  [BSI] : Incorporated feedback and provided revision 1.  [Huawei] : fine with r1. |  |  |
|  |  | S3‑240004 | GSMA clarification: no unused functions | BSI(DE) | CR | [Nokia] : clarification is required for terms, e.g., functions, etc.  [BSI] : Nokias request refers to the baseline, not the CR itself.  [Huawei] :Requires clarification.  [BSI] : will provide revision.  <CC1>  Michael presents  Comments already on email  Chair: comments contentious?  BSI: prefer not to revisit definitions, limit revisions to new text  Chair: restrict to GSMA comments, don't expand scope more than required  BSI: in general fine, but may be some low hanging fruit in some places  Chair: ok  E//: point 1, what was there before in this test case?  BSI: trying to clarify the concept of function  E//: note 2 and 3 for making easier for tester?  BSI: yes  E//: addition of hardware in result  BSI: more for completeness  Nokia: also asking on hardware perspective, what does this mean from product perspective, when there is redundancy does this mean unplugging things  DCM: make clear that there is documentation of the functionality, I don't see unplugging required, this contribution is clarification, more updates separate CR  Nokia: send update on email if required  E//: is this addressing GSMA input?  BSI: yes  Oppo: clarification of undocumented hardware – not mentioned by GSMA, should this be reflected back to GSMA?  Chair: this would make it a big topic  DCM: maybe separate hardware and software in a future description of the test case  Mitre: if SA3 feels it is required, SA3 should do it  Chair: concrete comments in email  </CC1>  [MITRE] : Editorials - please check the styles and the baseline document that was used for the CR.  [BSI] : Incorporated feedback and provided revision r1  [Huawei] : request a further change.  [BSI] : provides revision 2 implementing requested changes of huawei |  |  |
|  |  | S3‑240005 | GSMA clarification: no unsupported components | BSI(DE) | CR | [Nokia] : clarification is required for terms, e.g., component,  [BSI] : Nokias request refers to the baseline, not the CR itself.  [Huawei] :Requires clarification.  [BSI] : will provide revision.  CC1>  Michael presents  Mitre: there may be an issue with COTS hardware  BSI: vendor needs to ensure lifetime support  Nokia: comments will be on email  E//: here clarifies that component list is in documentation, is that the case  DCM: does that mean SBOM?  Chair: hardware not included in SBOM  DCM: agree  BSI: SBOM and generic description "components" on hardware side  </CC1>  [BSI] : Incorporated feedback and provided revision 1.  [Huawei] : request a further change.  [BSI] : provides revision 2 implementing requested changes of huawei  <CC4>  Huawei: reply in email, it's ok  E//: software libraries and hardware components are available – discussion was to take it out  BSI: ok, remove it in the revision  </CC4> |  |  |
|  |  | S3‑240006 | GSMA clarification: File system Authorization privileges | BSI(DE) | CR | [Nokia] : clarification is required for term 'authorization privilege'  [BSI] : Nokias request refers to the baseline, not the CR itself.  [Huawei] :Requires clarification.  [BSI] : will provide revision.  <CC1>  Michael presents  No comments  </CC1>  [MITRE] : Does the 'Expected evidence' section need further additions?.  [BSI] : Incorporated feedback and provided revision r1 |  |  |
|  |  | S3‑240007 | Correct RRC connection reconfiguration to RRC reconfiguration | Qualcomm Incorporated | CR | <CC1>  Adrian presents  QC: 0031 makes technical changes, overlapping, may need to merge into 0031  Discussion moved to 0031  </CC1> |  |  |
|  |  | S3‑240008 | Test Case on Password Storage Support | Nokia, Nokia Shanghai Bell, BSI | CR | CC1>  Sawros presents  Mitre: shouldn't we define non broken rather than remove it  Nokia: easier solution  Mitre: may be wrong baselinie  Nokia: changes are not affected by update to 18.2, will create update  Chair: can this be done by Mirko?  Nokia: need a revision  Huawei: not agreed in GSMA, just Nokia input?  Nokia: correct not related to GSMA input  DCM: dictionary and rainbow table should be considered separate attacks  Mitre: not specific to Rainbow tables, about data in storage  </CC1>  [Nokia] is sharing revision 1 of S3-240008  [Nokia] clarification for attack types  <CC3>  Nokia: usage of non-broken is put back into the revision, dictionary and rainbow attack are different, so only rainbow is taken into consideration  Huawei: ok with leaving out dictionary  E//: need to show the baseline changes for baselinie reference  DCM: dictionary attacks still relevant, need bcrypt  Nokia: disagree, offline only rainbow table attacks need to considered, not attack with plaintext  Chair: Please work offline to arrive at proper text, excluding any attack types was not the intention of the contribution.  </CC3>  [Nokia] is sharing revision 2, with reintroduced dictionary attack  [Huawei] fine with r2 and comments on the relevance of which attack  <CC4>  Nokia: r2 available  Huawei: ok with revision  DCM: ok  E//: editorial cleanup required, show that dictionary attack was existing previously  </CC4> |  |  |
|  |  | S3‑240009 | Test Case on No Default Content | Nokia, Nokia Shanghai Bell | CR | [BSI] : terms, version, pre-condition, typo, evidence  [Huawei] does not agree with this contribution in its current form due to the extent of changes and lack of justification.  [Nokia] is providing response to all comments  [Huawei] proposes to convert and merge this in a draft CR to be used as a living documents until all the changes are properly discussed, refined and agreed.  [Nokia] : is providing revision 1 of S3-240009 to 240013  <CC2>  Stawros presents r1  E//: new things added as evidence why added this?  Nokia: addressing a comment  BSI: more evidence is necessary, logfile not sufficient  E//: this is more something from documentation, not really test output, maybe not so good idea  BSI: ok to remove vendor documentation  Huawei: sent comments, too, now too many changes, convert to draft CR, as TS are in use, changes need to be carefully reviewed, merge all the changes into one draft CR  Mitre: helpful if the feeling is it is going beyond cat F, please point out exactly where it is cat B.  E//: because there is a phase 3 WID, we could turn those CRs into draft CRs, but if that was not limited to those, then revert this proposal  Chair: multiple documents or single document?  Huawei: yes  Stawros: can put all 5 proposals into one document, but what is the problem with the current revision  DCM: what constitutes a feature in SCAS?  Continue on email  Huawei: subjectivity and clarification questions could be addressed, just need more time  Chair: how to address the GSMA comments?  Huawei: only relevant for March plenary  DCM: need to be wary of time issue  GSMA: specific comments are relevant, but GSMA tried to be general in their comments, and those comments are the minimum, and the result should make the regulators happy. Also encourage improvements of other test cases.  Oppo: focus on essential changes for tis meeting, other for before next meeting  Huawei: why needs device under test needs to be added to this test case only? Just an example in this document  Nokia: make a lightweight version, discuss tomorrow, and see where it going  Huawei: ok with this proposals  </CC2>  [Nokia] is sharing revision 2, based on the agreements from our meeting yesterday (Day#2)  [Huawei] still disagrees with the changes to the test.  [Nokia] would like to understand why the proposed changes 'are completely modifying the test'  [Huawei] replies  [Nokia] is sharing revision 3, based on feedback from Huawei, and is also introducing new proposed text on the pre-condition for automated assessment tool  <CC4>  Nokia: provides r3  Huawei: will confirm by email, also affects other documents  Nokia: if ok, will update the other documents likewise (10, 11, etc)  </CC4> |  |  |
|  |  | S3‑240010 | Test Case on No Directory Listings | Nokia, Nokia Shanghai Bell | CR | [BSI] : terms, version, evidence, questions, typo  [Huawei] does not agree with this contribution in its current form due to the extent of changes and lack of justification.  [Nokia] is providing response to all received comments  [Huawei] proposes to convert and merge this in a draft CR to be used as a living documents until all the changes are properly discussed, refined and agreed.  [Nokia] is sharing revision 2, with changes as agreed in yesterday's meeting (Day#2)  [Huawei] still disagrees with the changes to the test. |  |  |
|  |  | S3‑240011 | Test Case on No Web Server Header Info | Nokia, Nokia Shanghai Bell | CR | [BSI] : terms, version, evidence, questions, typo  [Huawei] does not agree with this contribution in its current form due to the extent of changes and lack of justification.  [MITRE] Looks good, needs some editorial fix's and the cover sheet could be improved.  [Nokia] is providing responses to all received comments  [Nokia] is responding to the MITRE feedback  [Huawei] proposes to convert and merge this in a draft CR to be used as a living documents until all the changes are properly discussed, refined and agreed.  [Nokia] is sharing the revision 2 of the document, with changes as agreed during the meeting yesterday (Day#2)  [Huawei] still disagrees with the changes to the test. |  |  |
|  |  | S3‑240012 | Test Case on No Web Server Error Pages Info | Nokia, Nokia Shanghai Bell | CR | [BSI] : terms, version, evidence, questions, typo  [Huawei] does not agree with this contribution in its current form due to the extent of changes and lack of justification.  [Nokia] is responding to all comments  [Huawei] proposes to convert and merge this in a draft CR to be used as a living documents until all the changes are properly discussed, refined and agreed.  [Nokia] is sharing the revision 2 of the document, with changes as agreed during the meeting yesterday (day#2)  [Huawei] still disagrees with the changes to the test. |  |  |
|  |  | S3‑240013 | Test Case on No Web Server File Type Mappings | Nokia, Nokia Shanghai Bell | CR | [BSI] : terms, version, pre-condition, evidence  [Huawei] does not agree with this contribution in its current form due to the extent of changes and lack of justification.  [Nokia] is responding to all comments  [Huawei] proposes to convert and merge this in a draft CR to be used as a living documents until all the changes are properly discussed, refined and agreed.  [Nokia] : is providing revision 1 of S3-240009 to 240013  [Nokia] is sharing the revision 2 of the document, with changes as agreed in our meeting yesterday (day#2)  [Huawei] still disagrees with the changes to the test. |  |  |
|  |  | S3‑240014 | Assessment tool definition | Keysight Technologies UK Ltd | CR | <CC2>  Antonio presents  Keysight: needs to review  ??: category D correct?  DCM: should be F  E//: is this automatic?  Keysight: yes  Chair: provide text if not ok  </CC2>  [Keysight]: Changed category from D to F in r1  [Nokia]: is commenting on the definition of the term 'Automatic assessment tool'  [Keysight]: Respond to Nokia  [Nokia]: is providing a suggestion for definition of 'Automated Assessment Tool'  [Keysight]: Respond to Nokia and new proposal  [Nokia]: is responding the updated proposal from Keysight  [MITRE] provides suggestion for definiton.  [Keysight]: Proposal merging MITRE and Nokia definitions  [Nokia]: is providing feedback to the latest proposal  [MITRE] fine with proposed text.  <CC4>  E//: affects other docs like 0066, on 0066: no normative language if it is optional  Nokia: should is optional  DCM: also add which assessment tool was used  Keysight: add to expected result  DCM: maybe add in one place?  E//: formulation with Nokia proposal 008 not aligned  Keysight: agreed in meeting this way  Huawei: separate CR, leave for next meeting  E//: ok, but maybe definition is interpreted as one global tool  Keysight: the understanding is to use different tools.  Mitre: tool can be used for different purposes  </CC4> |  |  |
|  |  | S3‑240015 | Discussion Paper on PCF SCAS contents | BSI(DE) | discussion | <CC2>  Jörg presents  E//: what should be outcome  BSI: agree that even without specific test cases can reach 80%  E//: normally rapporteur just says whether 80% has been reached  Chair: yes  Huawei: so no annex about PCF to 33.926  Oppo: at 80% send to plenary for information  DCM: just make it ready for sending for approval  </CC2> |  |  |
|  |  | S3‑240016 | Improving the SCAS specification way of work | Nokia, Nokia Shanghai Bell | discussion | [BSI] : clarification required for Observation 2 and 3, objection of recommendation (R2) and (R3) in this strict form  [Huawei] provides comments  <CC2>  Stawros presents  Huawei: agree with some of the observation, need an SPD, convert 0015 to annex to 926 to address Nokias concerns  E//: inline with discussion in last couple of meetings, often 117 test cases cover everything  BSI: without specific document, it is difficult to add specific cases  GSMA: not ok recommendation 2 – no risk analysis has been done, only threat analysis, not ok to endorse as is  Nokia: that is correct, risk analysis has not been done as implementation specifc, in R2 should refer to threat analysis  E//: threat analysis is sufficient  Huawei: can't endorse on the fly  </CC2>  [Nokia] : is providing response to BSI  [Nokia] provides response to Huawei |  |  |
|  |  | S3‑240017 | Minimized kernel network functions (TC\_IP\_MULTICAST\_HANDLING) | Deutsche Telekom AG | CR | MCC made comments on the cover page (wrong WID used, no summary of the changes) and the body of the CR (missing clause header).  <CC2>  Johannes presents  DCM: change of test case (forward vs listen), difference IPv4 and IPv6, will send update by email  The contribution needs major revisions.  DT provides and updated version in the draft folder with changes proposed for the cover sheet and reproducing the whole clause. However, as the request from NTT DoCoMo is a very valid one, but requires major changes, we propose to note the document and come back addressing those major changes at the next meeting.  <CC4>  DT: note document, make it better for next meeting.  DCM: will help with CR for next meeting  </CC4> |  |  |
|  |  | S3‑240018 | No automatic launch of removable media[TC\_NO\_AUTO\_LAUNCH\_OF\_REMOVABLE\_MEDIA] | Deutsche Telekom AG | CR | [BSI] comments on header, test name, requirement name  <CC2>  Johannes presents  No comments  </CC2>  [DT] provided r1 to incorporate the proposed changes |  |  |
|  |  | S3‑240019 | Syn Flood Prevention[TC\_SYN\_FLOOD\_PREVENTION] | Deutsche Telekom AG | CR | MCC made comments on the cover page (wrong WID used, no summary of the changes) and reminded that no comments on the body of the text were allowed.  <CC2>  Johannes presents  DCM: large is unspecified, needs to be something else, e.g. line rate?  Keysight: use numbers from previous attacks, provide on email  </CC2>  [Keysight] : propose new text for the number of packets in r1  [Huawei] : cannot accept r1  [DT] DT appreciates the efforts from Keysight to improve the text! We have checked internally and we are fully in line with and support the proposed wording!  <CC4>  Huawei: commented to r1  Keysight: what was the problem?  DT: DT was ok with the proposal, Huawei was not ok, DT proposal to say how huge number is calculated in note.  Huawei: almost aligned with Huawei, see new version  Kesight will make revision  DCM: line speed is massive, maybe this is too much.  Huawei: ok with note  DT: need a formula for the testers  Huawei: agree with large quantity must be defined  E//: maybe half the link speed should be added in the note  DCM: add in the evidence which link speed was used  DT: too many changes discussed, just turn into note.  </CC4> |  |  |
|  |  | S3‑240020 | External filesystem mount restrictions(TC\_EXTERNAL\_FILE\_SYSTEM\_MOUNT\_RESTRICTIONS) | Deutsche Telekom AG | CR | [Nokia] : clarification is required for term 'suitable privilege escalation'?  MCC made comments on the cover page (wrong WID used, no summary of the changes) and the body of the CR (comments need to be removed).  <CC2>  Johannes presents  DCM: add examples for common operating systems for suitable privilege escalation method  Huawei: maybe not social engineering, something else?  </CC2> |  |  |
|  |  | S3‑240026 | Clarification of bootable memory device test | BSI(DE) | CR | [Huawei] : request a revision.  <CC2>  Michael presents  Huawei: had email exchange  E//: evidence: coming back to documentation stuff  DCM: make documentation part of evidence should be general and in Phase\_3  </CC2>  [BSI] : response to huawei.  [BSI] : provided revision 1 with incorporated feedback of discussion |  |  |
|  |  | S3‑240027 | Clarification of UP Integrity Protection test cases for eNB | BSI(DE) | CR | <CC2>  Michael presents  </CC2> |  |  |
|  |  | S3‑240028 | Clarification of UP IP selection and bidding down prevention of eNB | BSI(DE) | CR | <CC2>  Michael presents  </CC2> |  |  |
|  |  | S3‑240029 | Added parameters to NRF discovery authorization | BSI(DE) | CR | MCC commented that this was not a correction, the category should be B. References to TS 33.501 were missing as well.  <CC2>  Michael presents  </CC2>  [Huawei] : request revision for the flexibility.  [Ericsson] : propose to postpone and wait for the clarifications of the normative text.  [BSI] : will postpone CR |  |  |
|  |  | S3‑240030 | Added parameters to NRF discovery authorization threat reference | BSI(DE) | CR | <CC2>  Michael presents  E//: comment applies to this and previous, need to wait one meeting cycle, work ongoing in 33.501, to be done in next SA3 meeting  BSI: would the test case become redundant, or just for sync?  E//: they might not be in synch  Huawei: big changes, cat B, ok with E// proposal, or make them draft CRs, add threat as new, refer to CT4 spec, and not quote verbatim  Chair: comments also over email, please  Dcm: just reference Note 12, so no quotation of text  </CC2>  [Ericsson] : propose to postpone and wait for the clarifications of the normative text.  [BSI] : will postpone CR |  |  |
|  |  | S3‑240031 | ClarificationandsimplificationoftestcasesregardingUPCPandIPactivationatsplit-gNB | BSI(DE) | CR | <CC1>  Michael presents  QC: deletion of "or not needed" needs to be aligned with gNB specification  QC: why is only RRC ciphering is crossed out  BSI: take this offline, believe it is aligned with gNB  QC: crossing out of decryption, because it is implicit?  DCM: regarding "or not needed" clarify whether up to tester or two test cases.  Chair: continue on 31  </CC1>  [Qualcomm]: provides comments on the CR  [Huawei]: we will do the alignment to gNB SCAS  [BSI]: comments on QC  [Qualcomm]: provides some responses  [BSI]: provides revision 1  [Huawei]: propose a way forward.  [BSI]: provides revision 2 and comments on Huawei  [Qualcomm]: provides an r3  <CC4>  BSI: r3, seems to be ok  </CC4> |  |  |
|  |  | S3‑240032 | ClarificationoftestcasesonuserdataIPandCPinsplit-gNB | BSI(DE) | CR | <CC2>  Michael presents  </CC2> |  |  |
|  |  | S3‑240033 | Removal of note in GVNP life cyle management | BSI(DE) | CR | <CC2>  Michael presents  Huawei: justification is not clear, the note should take care of proprietary interface, original requirement  BSI: understand the limitation better  DCM: proprietary is not ok, should be about internal  E//: Note should be in applicability  </CC2>  [Huawei]: finds the contribution is not acceptable in current form and ask for more justification for removal of this NOTE.  [Ericsson]: Thinks that the NOTE should be moved to Pre-Condition part.  [BSI] : provided revision 2 with incorporated feedback and extensive justification |  |  |
|  |  | S3‑240034 | Fixed typo in VNF traffic separation testcase | BSI(DE) | CR | <CC2>  Michael presents  DCM: should be cat D  </CC2>  [BSI] : provided revision 1 with correct category on cover sheet (F-}D) |  |  |
|  |  | S3‑240035 | Clarifications to Basic Vulnerability testcases | MITRE Corporation | CR | [Nokia] : clarification required on the duration time of the fuzzing  [Huawei] finds the contribution not acceptable in its current form due to lack of justification and requires retaining only changes related to the reference document (discussed in SA3#113) for now.  [MITRE] provides r1 with justification in cover sheet and addresses comments from Nokia and Huawei  <CC2>  David presents  </CC2>  [Ericsson] provides comments.  [MITRE] provides clarification.  [Ericsson]: requests for clarifications.  [Nokia] provides comments.  [Huawei] supports Nokia and Ericsson comments  <CC4>  Mitre: will send revision shortly  Huawei: please remove changes over changes  Mitre: will be cleaned up for r4  Nokia: for many CVEs there are no PoCs available, so it is difficult to do this test for "all"  E//: agree with Nokia  Mitre: will address this comment, provide minimal version  E//: vulnerabilities could be documents, could be way format, maybe document which CVEs were tested, do this next meeting.  </CC4> |  |  |
|  |  | S3‑240036 | Update to the clause 4.2.2.2.2-Protection at the transport layer | Samsung | CR | [Samsung] : provides r1  <CC2>  Rajvel presents r1  </CC2>  [MITRE] : Asks why this CR is needed, does section 4.2.2.2.1 Introduction not already state its applicable to SBI  [Ericsson] : Provides comments  [Ericsson] : Provides reformulation of the proposed text.  [Huawei] : Provides reformulation of the proposed text based on Ericsson's proposal.  [Samsung] : provides r2 based on the text proposal from Ericsson and Huawei. Further provides clarification on the need for the CR  [Ericsson] : requests for clarifications  [Huawei] :Reply to Ericsson  [Samsung] : provides r3 and clarification  <CC4>  Samsung: presents revesion  Huawei: new sentence should be a note  E//: ok  Samsung: ok  </CC4> |  |  |
|  |  | S3‑240037 | Update to the clause 4.2.3.2.4-Protecting data and information in transfer | Samsung | CR | [Samsung] : provides r1  <CC2>  Rajvel presents r1  E//: Comment on cover sheet  E//: just publicly available SSH profile, that is still subjective  Chair: how to resolve this, maybe list some examples from SDOs?  DCM: removing is not making it better, giving examples is better.  </CC2>  [Ericsson] : provide comments  [Samsung] : provides r2 based on the way forward proposed during the Conf Call#2 |  |  |
|  |  | S3‑240038 | Update to the clause 4.2.3.3.2-Boot from intended memory devices only | Samsung | CR | [Samsung] : provides r1  [BSI] : request revision  [Samsung] : provides r2 based on the comments from BSI.  <CC2>  Rajvel presents r2  </CC2> |  |  |
|  |  | S3‑240039 | Update to the clause 4.2.3.4.1.1-System functions shall not be used without successful authentication and authorization | Samsung | CR | [Samsung] : provides r1  <CC2>  Rajvel presents r1  </CC2> |  |  |
|  |  | S3‑240040 | Updatetotheclause4.2.3.4.3.1-PasswordStructure | Samsung | CR | [Samsung] : provides r1  <CC2>  Rajvel presents r1  E//: WID code change?  </CC2> |  |  |
|  |  | S3‑240041 | Updates threat references to TS33.117-clauses4.2.2to4.2.3 | ZTE Corporation | CR | <CC2>  Peilin presents 0041-0048, changes are too long hence split in to 6 files.  Mitre: coversheet update to why these changes are needed  E//: was discussed in Chicago, so thank you for doing the work  Michael: is the editor's note true?  Mitre: are threat references examples or exclusive  ZTE: just example  </CC2>  [MITRE] : requests changes to threat references and more justification in cover sheet  [ZTE] : provide r1  [MITRE] fine with r1 |  |  |
|  |  | S3‑240042 | Updates threat references to TS33.117-clauses4.2.4to4.2.6 | ZTE Corporation | CR | [MITRE] : requests changes to threat references and more justification in cover sheet  [ZTE] : provide r1  [MITRE] fine with r1. |  |  |
|  |  | S3‑240043 | Updates threat references to TS33.117-clauses4.3.2 | ZTE Corporation | CR |  |  |  |
|  |  | S3‑240044 | Updates threat references to TS33.117-clauses4.3.3 | ZTE Corporation | CR |  |  |  |
|  |  | S3‑240045 | Updates threat references to TS33.117-clauses4.3.4 to4.3.5 | ZTE Corporation | CR | [MITRE] : requests changes to threat references and more justification in cover sheet  [ZTE] : provide r1  [MITRE] provides further comments and will be fine with the r2 with one change  [ZTE] : provide r2 |  |  |
|  |  | S3‑240046 | Updates threat references to TS33.117-clause4.4.2to4.4.4 | ZTE Corporation | CR | [MITRE] : requests changes to threat references and more justification in cover sheet  [ZTE] : provide r1  [MITRE] fine with r1 |  |  |
|  |  | S3‑240047 | Changes to 4.2.4.1.2.1 | Huawei; HiSilicon | CR | <CC2>  He presents, straightforward changes addressing GSMA comments, Tdocs 47-51.  <CC2>  [Ericsson]: proposes changes  [Huawei]: provide r1 |  |  |
|  |  | S3‑240048 | TS33.117\_Changesto4.2.4.2.2 | Huawei, HiSilicon | CR | [Huawei]: provide r1 in which a meaningful title in the cover is provided. |  |  |
|  |  | S3‑240049 | TS33.117\_Changesto4.2.5.3 | Huawei, HiSilicon | CR | [Huawei]: provide r1.  [Qualcomm] editorial change requested  [Huawei] provide r2  [Qualcomm] r2 OK |  |  |
|  |  | S3‑240050 | TS33.117\_Changes to 4.2.6.2.1 | Huawei, HiSilicon | CR | [Huawei]: provide r1 in which a meaningful title in the cover is provided. |  |  |
|  |  | S3‑240051 | Changes to 4.3.2.1 | Huawei ;HiSilicon | CR | [Ericsson]: Provides comments.  [Huawei]: provide r1. |  |  |
|  |  | S3‑240052 | Changesto4.2.2.1.8inTS33.511 | Huawei; HiSilicon | CR | <CC2>  He presents  </CC2>  [Huawei]: provide r1 in which a meaningful title in the cover is provided. |  |  |
|  |  | S3‑240053 | Changesto4.2.2.1.12inTS33.511 | Huawei; HiSilicon | CR | <CC2>  He presents  </CC2>  [Huawei]: provide r1 in which a meaningful title in the cover is provided.  [Qualcomm] editorial change needed  [Huawei]: provide r2  [Qualcomm] r2 OK |  |  |
|  |  | S3‑240054 | TS33.117\_Changesto4.2.2.2.2 | Huawei, HiSilicon | CR | <CC2>  He presents  DCM: could be cat D  </CC2>  [Huawei]: provide r1 in which a meaningful title in the cover is provided.  [Ericsson]: provides comments |  |  |
|  |  | S3‑240055 | AddcertificateenrolmenttoTS33.511 | Huawei; HiSilicon | CR | MCC commented that this should have been cat-B (not a correction) and that clause 2 was missing from the clauses affected section on the cover page.  [Ericsson]: This test seems to be functional test, not security one.  <CC3>  [Huawei] presents.  [Ericsson] comments on 055 and 056. It seems like functional test rather than security test.  [BSI] supports this. There are so many functional tests in this area.  [Huawei] replies.  </CC3>  [Ericsson]: proposes to note this document, as the proposal appears to be more functional test than security test.  <CC4>  E//: propose to note as said previously, as it is functional test  Huawei: ok to note for now  </CC4> |  |  |
|  |  | S3‑240056 | PeercertificatecheckingatgNBtoTS33.511 | Huawei; HiSilicon | CR | MCC commented that this should have been cat-B (not a correction).  [ERICSSON]: This test seems to be functional test, not security one.  <CC3>  [Huawei] presents.  </CC3>  [Ericsson]: proposes to note this document, as the proposal appears to be more functional test than security test.  <CC4>  E//: propose to note as said previously, as it is functional test  Huawei: ok to note for now  </CC4> |  |  |
|  |  | S3‑240057 | Add threat to certificate enrolment | Huawei; HiSilicon | CR | [Ericsson]: This is related to CMPv2 and it is a threat that points to a functional test ( the one proposed in S3-240055 {https://www.3gpp.org/ftp/TSG\_SA/WG3\_Security/TSGS3\_114e/Docs/S3-240055.zip} )  <CC3>  [Huawei] presents that is threats related so it can be skipped.  </CC3>  [Ericsson]: Proposes to note this proposal as it is related to CMPv2 implementation, and it is a threat that points to a functional test (the one proposed in S3-240055 {https://www.3gpp.org/ftp/TSG\_SA/WG3\_Security/TSGS3\_114e/Docs/S3-240055.zip} )  <CC4>  E//: propose to note as said previously, as it is functional test  Huawei: ok to note for now  </CC4> |  |  |
|  |  | S3‑240058 | Add threat to peer certificate checking at gNB | Huawei; HiSilicon | CR | MCC commented that this should have been cat-B (not a correction).  [Ericsson]: This is related to certificate checking and it is a threat that points to a functional test (the one proposed in S3-240056 {https://www.3gpp.org/ftp/TSG\_SA/WG3\_Security/TSGS3\_114e/Docs/S3-240056.zip} )  <CC3>  [Huawei] presents that is threats related so it can be skipped.  </CC3>  [Ericsson]: Proposes to note this proposal as it is related to the functionality of checking certificate validity, and it is a threat that points to a functional test (the one proposed in S3-240056 {https://www.3gpp.org/ftp/TSG\_SA/WG3\_Security/TSGS3\_114e/Docs/S3-240056.zip} )  <CC4>  E//: propose to note as said previously, as it is functional test  Huawei: ok to note for now  </CC4> |  |  |
|  |  | S3‑240059 | Test case update to TS33.511 | Huawei; HiSilicon | CR | [Nokia] : clarification required on the reduced/restricted logging  [Huawei] : reply to Nokia to ask clarification on the question.  [Nokia] is answering the question from Huawei  [Huawei] : reply to Nokia.  [Qualcomm]: makes comment  [Huawei] : reply to QC.  [Qualcomm]: OK with r1  <CC3>  [Huawei] presents there is r1 and Qualcomm is ok to r1 now.  </CC3> |  |  |
|  |  | S3‑240060 | Correction to TS33.511 | Huawei, HiSilicon | CR | [Huawei]: provide r1  <CC3>  [Huawei] presents.  </CC3> |  |  |
|  |  | S3‑240061 | [mirror]correction to TS 33.511 | Huawei, HiSilicon | CR | <CC3>  (mirror)  </CC3> |  |  |
|  |  | S3‑240062 | [mirror]correction to TS 33.511 | Huawei, HiSilicon | CR | <CC3>  (mirror)  </CC3> |  |  |
|  |  | S3‑240063 | Clarificationfor4.3.4.2-33.117 | Keysight Technologies UK Ltd | CR | MCC commented that this CR should have a rel-18 SCAS WID (e.g, SCAS\_5G\_Ph3). eSCAS\_5G belongs to Rel-17. Also on the cover page, source to TSG: S3.  [Keysight]: Provides revision  <CC3>  Antonio presents  Huawei: other CRs are doing the same change, but not in aligned fashion, better to have same changes everywhere  Keysight: can take the action  Nokia: CR0014 is defining what is automatic assessment tool, in many test cases this recommendation exists, but try to reexplain assessment tool, just say recommendation: use a tool  Chair: Antonio holds the pen, make it uniform.  Huawei: if definition converges, then each author of contributions that are changing the recommendation just removes this change. Align for next meeting.  Chair: not have much time in next meeting, so better to align in this meeting  Nokia: in recommendation say: "use automatic assessment tool".  Oppo: if automatic assessment tool is not available, then what?  Huawei: use own skills, maybe keep the rest  Nokia: the whole line is not adding value, that is test lab decision.  Huawei: just converge on definition for now, and GSMA comments should be addressed  Nokia: let's keep recommended, and write automatic test tool  E//: maybe better to remove the recommendation, then maybe clarify in TTCN3  Mitre: what do the requirements specify?  Huawei: why keep this or not, why modify it?  Keysight: maybe ok to leave as is  Tmobile: text seems strange,  DCM: maybe the issue is with closed source assessment tools where it is not clear what exactly has been tested for.  E//: take it out now, and clarify later on.  Chair: is there a definition in 0014  Keysight: current state: A software system that aids the user in evaluation of the security of computer programs, systems and/or networks  Nokia: competing proposal posted, by defining the individual parts: automatic, assessment, and tool: "Automatic Assessment Tool: “An Automatic Assessment Tool is a software component(?) that is operating with minimal human intervention and is performing/running a series of planned tests with the aim to determine how secure the system under test is."  Chair: converge on definition and not touch the existing recommendation  Tmobile: "from NIST Tool Configuration: A recommendation for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information"  </CC3>  <CC4>  Keysight: agreed to remove the recommendation, no comments  E//: looks ok  </CC4> |  |  |
|  |  | S3‑240064 | AddclarificationstoTS33.511 | Huawei; HiSilicon | CR | [Huawei]: provides r1 |  |  |
|  |  | S3‑240065 | AddclarificationstoTS33.511 | Huawei; HiSilicon | CR | MCC commented that this should have been cat-F with the WID code eSCAS\_5G (SCAS WID for Rel-17).  [Huawei]: reply to MCC, and provide r1 |  |  |
|  |  | S3‑240066 | Clarificationfor4.3.4.3-33.117 | Keysight Technologies UK Ltd | CR | [MITRE]: requests minor changes  [Ericsson]: provides comments.  MCC asked to change the WID on the cover page to SCAS\_5G\_Ph3, add S3 as source for TSG.  [Keysight]: Response to MITRE, Ericsson and MCC  [MITRE] provides suggestion.  <CC3>  Antonio presents  Mitre: comment on email, nothing major  </CC3>  [Nokia]: kicks off the discussion on the text of 'Recommended: an automated assessment tool...'  [Ericsson]: requests for clarifications for the original document and provides opinion on the automatic test tool. |  |  |
|  |  | S3‑240067 | Log transfer to centralized storage | Ericsson | CR | [BSI] points to a small editorial glitch  <CC3>  Markus presents  Continue on email  </CC3>  [Ericsson] editorial glitch fixed in revision 2 |  |  |
|  |  | S3‑240068 | Growing content shall not influence system functions | Ericsson | CR | <CC3>  Markus presents  </CC3> |  |  |
|  |  | S3‑240069 | Processing of ICMPv4 and ICMPv6 packets | Ericsson | CR | CC3>  Markus presents  Mitre: changes in document are more than what is given in reason for change  </CC3> |  |  |
|  |  | S3‑240070 | Handling of IP options and extensions | Ericsson | CR | [MITRE] requests minor change  [Qualcomm] changed required  [MITRE] fine with r1  [Ericsson] r2 uploaded based on comments from the conference call  [MITRE] fine with r2.  <CC3>  Markus presents r1  QC: add [x] in the reference  E//: ok  </CC3>  [Qualcomm] r2 OK |  |  |
|  |  | S3‑240071 | Editorial Updates to Section 4.3.5.1 of TS 33.117 for clarification | IIT Bombay | CR | [Nokia] : clarification required on the term 'passes', is there a separation of egress and ingress traffic possible  [Huawei] comments on the changes  [IIT Bombay]: Responding to clarification on the term 'passes'  [IIT Bombay]: Incorporated feedback and provided revision r1  [Ericsson]: provides comments.  [IIT Bombay]: providing revision r2  [Huawei] disagrees with the changes to the execution steps.  [Nokia] : clarification required on the term 'passes', is there a separation of egress and ingress traffic possible  [Huawei] comments on the changes  [IIT Bombay]: Responding to clarification on the term 'passes'  <CC3>  Manjesh presents  Huawei: disagree change in execution step, GSMA only suggested change, so not mandatory to adopt  Nokia: problem with ingress and egress  Huawei: changes to execution steps can be problematic because it is in production  Nokia: understand what is the thinking, but need to weigh whether it is necessary  DCM: of with r2, but expected results are a bit unclear  Huawei: not fine with the changes to the execution steps, only creating confusion, ok with changing preconditions  Tmobile: can't use must  Oppo: move some text to Note in execution steps.  IITB: if test is already scripted, what is it doing, what should we assume.  </CC3>  [IIT Bombay]: Incorporated feedback and provided revision r3  <CC4>  IITB: present r3, should be ok, will clean up  </CC4> |  |  |
|  |  | S3‑240072 | EditorialUpdatestoSection4.3.6.2ofTS33.117forclarification | IIT Bombay | CR | [Nokia] : improvement required on the HTTP methods, i.e., change to HTTP requests  [Huawei] proposes changes  [IIT Bombay]: responding to suggestion on changing 'HTTP methods' to 'HTTP requests'  [MITRE] proposes some changes.  [IIT Bombay]: Incorporated feedback and provided revision r1  [Ericsson]: proposes changes.  [IIT Bombay]: providing revision r2  [Huawei] fine with r2  <CC3>  Manjesh presents  Mitre: fix styles  IITB: should be fixed  </CC3> |  |  |
|  |  | S3‑240073 | EditorialUpdatestoSection4.3.6.3ofTS33.117forclarification | IIT Bombay | CR | [IIT Bombay]: providing revision r1  [Ericsson]: proposes changes.  [IIT Bombay]: providing revision r2  <CC3>  No comments  E//: same discussion on machine/equipment as in 74  </CC3>  [IIT Bombay]: providing revision r3, tester machine changed to test equipment in pre condition  <CC4>  IITB: revision should be ok  E//: preconditions should not have normative language  </CC4> |  |  |
|  |  | S3‑240074 | EditorialUpdatestoSection4.3.6.4ofTS33.117forclarification | IIT Bombay | CR | [IIT Bombay]: providing revision r1  [MITRE] requests changes and clarifications  [IIT Bombay]: providing revision r2  [MITRE] fine with r2.  <CC3>  Manjesh presents  IITB: inconsistent use of terms tester machine and test equipment, what to use  Huawei: no need to change, hasn't been an issue  Chair: why using tester machine, in this test normally called test equipment  IITB: because that's what it's called in 33.117  Chair: stay with one term inside the test case.  </CC3>  [Huawei] proposes to soften the language in the preconditions.  [IIT Bombay]: Incorporating suggestions and providing r3  <CC4>  IITB: revision should be ok  E//: preconditions should not have normative language  </CC4> |  |  |
| 4.1.2 | Service Based Architecture |  |  |  |  |  |  |  |
| 4.1.3 | Security Aspects of Proximity based services in 5GSProSe |  |  |  |  |  |  |  |
| 4.1.4 | Mission Critical |  |  |  |  |  |  |  |
| 4.1.5 | Authentication and key management for applications based on 3GPP credentialin 5G |  |  |  |  |  |  |  |
| 4.1.6 | Enhancements to User Plane Integrity Protection Support in 5GS |  |  |  |  |  |  |  |
| 4.1.7 | Security AspectsofEnhancementsfor5GMulticast-BroadcastServices |  |  |  |  |  |  |  |
| 4.1.8 | Security for enhanced support of Industrial IoT |  |  |  |  |  |  |  |
| 4.1.9 | Security Aspects of eNPN |  |  |  |  |  |  |  |
| 4.1.10 | Security Aspects of Enhancementof Support for Edge Computingin 5GC |  |  |  |  |  |  |  |
| 4.1.11 | Security aspects of Uncrewed Aerial Systems |  |  |  |  |  |  |  |
| 4.1.12 | Security Aspects of Ranging Based Services and Side link Positioning |  |  |  |  |  |  |  |
| 4.1.13 | SecurityAspectsofeNA |  |  |  |  |  |  |  |
| 4.1.14 | ModifiedPRINSforroamingserviceprovidersin5G |  |  |  |  |  |  |  |
| 4.1.15 | All other maintenance topics (not listed above) |  |  |  |  |  |  |  |
| 4.2 | New WID on 5G Security Assurance Specification(SCAS) for the Unified Data Repository(UDR). | S3‑240021 | SecurityAssuranceSpecification(SCAS)fortheUnifiedDataRepository(UDR) | BSI(DE) | Draft TS | <CC1>  Jörg presents  Oppo: is a cover needed for this?  Chair: yes  BSI: draft TS  Mirko: is ok  </CC1>. |  |  |
|  |  | S3‑240022 | ScopedefinitionfordraftTS33.530 | BSI(DE) | pCR | <CC1>  Jörg presents  No comments  </CC1> |  |  |
|  |  | S3‑240023 | IntroductionfordraftTS33.530clause4 | BSI(DE) | pCR | <CC1>  E//: same text as scope, look at UDM text  BSI: ok, will update  </CC1>  [BSI] : is providing revision 1 of S3-240023  [Huawei] : Huawei is fine with r1. Thanks.  [Ericsson] : is fine with r1. |  |  |
|  |  | S3‑240024 | UDR-specificsecurityrequirementsandrelatedtestcasesfordraftTS33.530 | BSI(DE) | pCR | <CC1>  Jörg presents  No comments  </CC1>  [Huawei] : proposal on the internal interface. |  |  |
|  |  | S3‑240025 | DiscussionoftheprotectionmechanismofthepermanentkeyleavingtheUDRenvironment. | BSI(DE) | discussion | Agreement  <CC1>  Jörg presents  Nokia: already made a comment on email: TLS shall be used, why is it possible to have no security? On authorization security: two levels of security, what is the necessity here when data is anyway protected on first level  E//: discussion paper more on normative work, not on SCAS, TR33.845 was studying that, maybe revisit.  Huawei: if 33.541 needs to be revisited is a separate discussion not test case. In case of internal interface, is it applicable  BSI: yes  DCM: need to ensure that internal interfaces are not externally accessible  Huawei: meaning that the interface is not exposed  Nokia: if the person testing is sitting in front of the UDM is not seeing the UDR interface  </CC1>  [Nokia] : clarification required for the part under heading 'transfer security'  [Nokia] : clarification required for the part under heading 'authorization security'  [Huawei] : Clarification on the deployment mode of UDR.  [Nokia] is providing reference to discussion document on the different UDR architecture and implementation options  [Ericsson]: provides comments.  [BSI] : clarification for the part under heading 'authorization security'  [BSI] : answer to Huawei proposal on the internal interface.  [BSI] : answer to Clarification on the deployment mode of UDR.  [BSI]: answer the provided comments.  [Huawei] : Propose to Note this discussion paper.  [BSI] : answer to propose to Note this discussion paper. |  |  |
| 4.3 | NewWIDonSCASforRel-18featuresonexistingfunctions. |  |  |  |  |  |  |  |
| 4.4 | NewWIDon5GSecurityAssuranceSpecification(SCAS)fortheShortMessageServiceFunction(SMSF). | S3‑240075 | DiscussionofDiameterinterfaceatSMSFtodefinerequirementsforSecurityAssuranceSpecificationsforSMSF | IIT Bombay | discussion | <CC1>  Manjesh presents  Just discussion paper  Manjesh: just introducing diameter interface as an asset  E//: so no new requirement, requirement already exists in specs  Huawei: in general, there is no NDS IP support requirement for network products  Nokia: update to R17? How is the intrerworking with LTE R17 handled now that we are on R19  Huawei: no difference to other standards, as long as no new requirement is introduced  </CC1> |  |  |
|  |  | S3‑240076 | AddannexuretoSecurityAssuranceSpecification(SCAS)threatsandcriticalassetsin3GPPnetworkproductclassesspecifictoSMSF | IIT Bombay | CR | Approval  <CC1>  Manjesh presents  DCM: are all network product classes new annexes  Oppo: ok  Huawei: make draft CR first as living document, then later convert to CR together with SCAS TS  Huawei: is new threat on interface protection required? Already exists and sufficient, details on email  Huawei: asset and threat discussion should be separate. Currently no necessity of adding threat part  Mitre: is this work item allocated for R19?  Huawei: this work is R19  </CC1>  [Huawei] : Suggest to remove the threats on the interface protection.  [IIT Bombay]: seeking clarity on the suggestion  [Huawei] : provide clarification on the threats.  [IIT Bombay]: removing the threat section and providing r1  MCC commented that the WID on the cover page should be SCAS\_5G\_SMSF. Clauses affected should be Annex X (new) and summary of changes was missing. They added some other minor comments for the body of the CR.  [IIT Bombay]: Incorporated feedback and provided revision r2 |  |  |
|  |  | S3‑240077 | NewrequirementinSCASforSMSFdraftTS33.529 | IIT Bombay | pCR | <CC1>  Manjesh presents  Huawei: discussion paper clarifies that three options can be used, but not all options are implemented, need to consider this in the test cases, more on email  </CC1>  [Huawei] : request clarificaiton on the flexibility.  [IIT Bombay]: Agreeing to the suggested change  [Huawei] : fine with r1. Thanks. |  |  |
|  |  | S3‑240078 | SMSFSpecificSecurityrequirementandtestcasefordraftTS33.529 | IIT Bombay | pCR | <CC1>  Manjesh presents  Marcus: test case in 33.117 looks very similar, what is the difference?  Manjesh: there is a note here  Huawei: SMSF is not only network product that supports diameter, there are SCAS test available, so no need for specific test  Chair: reference specific test  Huawei: will send clause number by email  </CC1>  [Nokia] : clarification required on the execution steps  [Huawei] : request clarificaiton on the necessity.  [IIT Bombay]: Providing clarification on the necessity of the test case  [IIT Bombay]: providing clarifications to the queries  [Huawei] : Provide feedback.  [IIT Bombay]: Providing feedback on test case |  |  |