**3GPP TSG-SA3 6G Study Planning**

**Conference Calls, 6 – 7 August 2025**

**Source: Chair of 3GPP TSG SA WG3**

**Title: Document order and key proceedings**

**Document for: Information**

**Agenda Item: -**

## **Document Order:**

**Rajvel welcomes everyone – mode of operation: 3 minutes per company presentation, then questions.**

|  |
| --- |
| **Day 1: 6-Aug-2025** |
| 1 | AT&T | DP-AT&T-v1.pptxMike presentsDCM: is additional work beyond approvd PQC requiredATT: no, but need to be prepared, and take the results into account.Lenovo: what about SA1 security requirements?ATT: need to be considered tooOrange: not a work task, but a general statement in the objectivesATT: open for that proposalNokia: this is including the whole network, not just core?ATT: yesE//: approve study in December plenary or re-evaluateATT: should be done then, could also be done in twoE//: could approve parts in Sept, and rest in DecQC: part of the AI is on application above 3GPP scopeATT: need system controls in 6G system for security |
| 2 | VDF | DP-Vodafone 6G Security-v1.docxFlavio presentsOrange: on 2.4 why is NAS on PQC migration? PQC auth in the rest refers to core network entities, what is the meaning here in 2.4Flavio: in the context of distributed NASOrange: so it's about key distribution between nodes, then make a general statementNokia: what kind of alignment with GSMA is foreseen? 2Nd: 256 AEAD only for radio or also NAS? 3rd: privacy is limited to pseudonomizationVDF: 1: need to align with all GSMA activities 2: also for NAS 3: masking of use identifiers, continue what we are doing alreadyChair: too solution specificLenovo: need to refer to specific GSMA document number, why only encryption, is it ruling out integrity protection of AEAD?VDF: will be more specific, integrity is includedApple: also not clear what is the alignment, it should be high level; PQC also is referring also to symmetric crypto, generally on AS, NAS; also support PQC in SID, no WT required, privacy mechanism can be discussed during the studyVivo: what is the security review and checklist?VDF: independent security need tool to be able to review that we have done this correctly, AI features also need to be controlled in a standardized way.E//: this security checklistVDF: collect all information about the new featureE//: so it is a way of workingVDF: yesHuawei: what is the scope of an additional work task for PQC? NSA: security review gate sounds more like risk assessment, maybe remove the word gate as it sounds like we should drop insecure features |
| 3 | China Mobile | DP-China Mobile-v1.docx, WT-China Mobile-v1.docxXiaoting presentsE//: decentralized trust managemetn is in scope of GSMA, wait for them to make progress.CMCC: especially distribution of trust anchors need to be done in 3GPP, GSMA will focus on governance. GSMA expects some work from 3GPPHuawei: revisit cross certification mechanism, should be independent topicLenovo: there are also other proposals to address trust management, should that only cover inter netowrk or also RAN aspects?CMCC: WT 2 here fits more into core network 6G sid. |
| 4 | T-Mobile | WT-T-Mobile\_v1.docxMike presentsDCM: how much of this do you want only in 6G?Tmo: originally for 6G, would also be nice in 5GDCM: could also be G independentTmo: if not included, then it should be separateCMCC: WT2 and WT5 access management is not only for security reasons, there is a WID that already does this, need to widen scope; WT5, another topic on how to treat network security beyond NDS, consider in more general ways.Tmo: trying to be very general, WT2 needs to revisited especially for dynamic policy control, open to rewording, expansion or contractionCATT: WT2: what is scope of identity or definition, give an exampleTmo: offlineCATT: what is dynamically?Tmo: part of reaction, immediately restrict or revoke access to person if something being seenJHU: WT6: security monitoring entity,new function to integrate into architecture of just new API; WT2.1 gaps in existing SIM and eSIM, or is this about SIMless devices; W5.1: gaps in slice segmentation, whta issues are beign seen?Tmo: Sechand is already defining the security monitoring, need closed loop automation; on 2.1: need to look at how identities are defined, SIMs are being spoofed, especially in roaming interfaces; on 5.1: slices could be on microsegment, control what it is doing, btter control over devices in that environmentE//: could study SIEM, but what needs to be standardized? Process question: what is the time limit?Chair: initial plan was to give concrete proposals, then moderator could work on this, clarification questions can be done offline. Have direct comments on WTLenovo: WT 2 requirements are aligned with SA1 requirementsOrange: some things are not in scope of 3GPP, many work tasks with content, that need justificaiton and KI, so CMCC better approach |
| 5 | SKT | WT-SK telecom-v1.docxYunesong presentsLenovo: subscriber data breach is separate from FBS, both need to be studied independently, needs to be studied as part of trust management, relates to CMCC proposal. Any certification related aspects need to be studied together, not push under FBS, CATT: why is SUCI related to FBS issue?SKT: offlineVivo: FBS can be put into RAN related work task, not discuss together with roaming use caseChair: handle placement of separatelyApple: agree to study FBS and auth enhancement separatelyE//: similarDCM: 6G system SID content?SKT: general 6G study itemQC: FBS concern: what has changed since the previous two studies, can the UE always be perfectly configured, tradeoff between DoS on network and DoS on UEChair: what should be done?QC: not clear this needs to be rehashedLenovo: certification relates to too many PKI related wor tasksOrange: not have these extensive work tasks. All that is written here is in regard to 5G. Depends on how the security architecture is built, part of RAN security work taskSKT: customer is sensitive to security attacks, enhance the security protection to make premium security services |
| 6 | Deutsche Telekom | WT-DeutscheTelekom-v1.docxThomas presentsChair: part of 6G system?DT: anchor in 6G study to integrate it, or separate study, then it can move fasterCableLabs: can be part of study by CMCC, independent SIDE//: part of SBA core network security study, does this study gointo specific container technology, not really have visibility at this level, not clear how much can be standardized? Are other kind of identities required?DT: decouple from transport layer, not look at implementationVivo: can be merged into CMCC study, related to PKIHuawei: PRINS at application layer exists, need an anchor somewhere. Any idea of how to manage the identitiesDT: that is the studyNokia: more of implementation, not bring this into standard, good to study, part of SBA, not part of SBADT: not implementation specificCMCC: generally support this topic, also in decentraliezd trust, also cover intra PLMN case, DCM: service mesh relies on the identification and autentication away from web serviceDT: offline |
| 7 | China Telecom | WT-China Telecom-v1.docx, DP-China Telecom-v1.docJun presentsJHU: depends on SA2 architectureCT: can be in 6G study?Tmo: is this part of SA2?CT: yes, localized network is part of localized service deliveryE//: need to see SA2 work first before starting DCM: also need to see SA2 result first |
| 8 | JHUAPL | WT-JHUAPL-v1.docxGino presentsDCM: should this be done in GSMA, like IR.67JHU: part of the challenge is root of trust establishment, linkages to some future work, appropriate for SA3Nokia: interdomain, GSMA is the right entity, for intradomain do profilingJHU: IETF provides toolbox, specify how provide interoperator and intervendor interoperability |
| 9 | Charter | WT-Charter-v-1-0.docxAchari presentsCATT: missing other SA2 work tasksCharter: these are topics of interest to us, other tasks are also there, CATT: is data privacy part of data framework, or separate?Charter: that#s part of the discussion, should be expanded hereVivo: WT 2, third bullet is not interworkingCharter: add on from Charter, 3GPP access is there from the start, address both 3GPP and non-3GPP from the start from point of view of Charter, should be integral part of architectureNokia: what is secure migration, non 3GPP access also needs SA2 alignmentCharter: study will determine the details, interworking is well understood  |
| 10 | Samsung | DP-Samsung-v01.doc, WT-Samsung-v01.docxRohini presentsNokia: concern on indepent WT on false base station, know certain gaps exist, consider this an independent WTSamsung: want this under 6G umbrella SIDE//: similar comment, Wts very specific, could be part of AS security work task, general list of work tasks, some proposals point to SA1 TR, TR has potential requirements, TS are the real requirements. Then downstream groups select themselvesQC: agree with FBS comment, agree with E// on SA1 security requirements, if there is a problem with 5G then this is a general idea, not much progress on giving ourselves a tight study scopeApple: generally support this proposal, agree with comment on SA1 requirementsVivo: agree with Apple: WT4 and 1.2 overlapDCM: could this be combined with the SA2 SID descriptionChair: need to have this discussion in the actual SID discussion, want to give thisE//: what to do with RANTmo: also do more general security workATT: set TUs aside to address 6G system securityOppo: RAN groups discussion already raised MACce security considerationsChair: preference is to have separate work tasks, assign TUs per work tasksE//: tomorrow need to discuss the points below the table in agenda, how to proceed? Chair: 30 minutes is reserved for that. Most WPs already aligned, so things should move faster.QC: how will moderator be appointed?Chair: will be discussed tomorrow. Suresh is interested in holding the pen.Chair: close meeting, Cablelabs document moved to end of document presentation tomorrow at request of presenter. |
| 11 | CableLabs | WT-CableLabs-v1.docx |
| 12 | vivo | DP-vivo-v1.pptx, WT-vivo-v1.docx |
| 13 | LGE | WT-LGE-v1.docx |
| 14 | ZTE | WT-ZTE-v1.docx |

|  |
| --- |
| **Day 2: 7-Aug-2025** |
| 15 | CATT | WT-CATT-v1.doc, DP-CATT-v1.doc |
| 16 | Lenovo | DP-Lenovo-v1.pdf, WT-Lenovo-v1.docx |
| 17 | Nokia | WT-Nokia-V1.docx |
| 18 | Interdigital | WT-Interdigital-6G User Consent-v1.docx, WT-Interdigital-6G Enhanced NAS Security-v1.docx,WT-Interdigital-6G MAC Layer Security-v1.docx, WT-Interdigital-6G Data Plane Security-v1.docx |
| 19 | Xiaomi | DP-Xiaomi-v1.doc, WT-Xiaomi-v1.pdf |
| 20 | Qualcomm | DP-Qualcomm-v1.pdf |
| 21 | Ericsson | DP-Ericsson-v01.doc, WT-Ericsson-v01.doc |
| 22 | Cisco | DP-Cisco-v1.docx, WT-Cisco-v1.docx, WT-Cisco-v2.docx |
| 23 | Way forward discussion |

|  |
| --- |
| **Key proceedings** |
| 1. Each company will get strictly 3 minutes for presentation
 |
| 1. Delegates are encouraged to provide concrete comments on the proposed WTs
 |

|  |
| --- |
| **Key proceedings on the way forward discussions:** |
| 1. A moderator to be appointed to prepare the **6G System** SID
* Please note, being assigned a moderator shouldn’t be taken as having an influence on assignment of rapporteurs.
 |
| 1. Moderator to prepare a draft **6G System** SID
* Compiling the WT inputs from companies
1. Initiate discussion on the draft 6G System SID (by 11-Aug-2025, 15:00 UTC) and end the discussion (by 15-Aug-2025, 15:00 UTC)
* Need to decide whether to have the discussion via e-mail or NWM tool
 |
| 1. Moderator to submit the 6G System SID for SA3#123 meeting (before the contribution submission deadline)
* Incorporating possible comments/updates received during the discussion period
 |
| 1. Further discussion on the moderator submitted 6G SID will happen during the SA3#123 meeting for SA3 agreement
 |