**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.pptx  Mike presents  DCM: is additional work beyond approvd PQC required  ATT: no, but need to be prepared, and take the results into account.  Lenovo: what about SA1 security requirements?  ATT: need to be considered too  Orange: not a work task, but a general statement in the objectives  ATT: open for that proposal  Nokia: this is including the whole network, not just core?  ATT: yes  E//: approve study in December plenary or re-evaluate  ATT: should be done then, could also be done in two  E//: could approve parts in Sept, and rest in Dec  QC: part of the AI is on application above 3GPP scope  ATT: need system controls in 6G system for security |
| 2 | VDF | DP-Vodafone 6G Security-v1.docx  Flavio presents  Orange: 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 2.4  Flavio: in the context of distributed NAS  Orange: so it's about key distribution between nodes, then make a general statement  Nokia: what kind of alignment with GSMA is foreseen? 2Nd: 256 AEAD only for radio or also NAS? 3rd: privacy is limited to pseudonomization  VDF: 1: need to align with all GSMA activities 2: also for NAS 3: masking of use identifiers, continue what we are doing already  Chair: too solution specific  Lenovo: 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 included  Apple: 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 study  Vivo: 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 checklist  VDF: collect all information about the new feature  E//: so it is a way of working  VDF: yes  Huawei: 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.docx  Xiaoting presents  E//: 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 3GPP  Huawei: revisit cross certification mechanism, should be independent topic  Lenovo: 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.docx  Mike presents  DCM: how much of this do you want only in 6G?  Tmo: originally for 6G, would also be nice in 5G  DCM: could also be G independent  Tmo: if not included, then it should be separate  CMCC: 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 contraction  CATT: WT2: what is scope of identity or definition, give an example  Tmo: offline  CATT: what is dynamically?  Tmo: part of reaction, immediately restrict or revoke access to person if something being seen  JHU: 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 environment  E//: 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 WT  Lenovo: WT 2 requirements are aligned with SA1 requirements  Orange: 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.docx  Yunesong presents  Lenovo: 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: offline  Vivo: FBS can be put into RAN related work task, not discuss together with roaming use case  Chair: handle placement of separately  Apple: agree to study FBS and auth enhancement separately  E//: similar  DCM: 6G system SID content?  SKT: general 6G study item  QC: 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 UE  Chair: what should be done?  QC: not clear this needs to be rehashed  Lenovo: certification relates to too many PKI related wor tasks  Orange: 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 task  SKT: customer is sensitive to security attacks, enhance the security protection to make premium security services |
| 6 | Deutsche Telekom | WT-DeutscheTelekom-v1.docx  Thomas presents  Chair: part of 6G system?  DT: anchor in 6G study to integrate it, or separate study, then it can move faster  CableLabs: can be part of study by CMCC, independent SID  E//: 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 implementation  Vivo: can be merged into CMCC study, related to PKI  Huawei: PRINS at application layer exists, need an anchor somewhere. Any idea of how to manage the identities  DT: that is the study  Nokia: more of implementation, not bring this into standard, good to study, part of SBA, not part of SBA  DT: not implementation specific  CMCC: 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 service  DT: offline |
| 7 | China Telecom | WT-China Telecom-v1.docx,  DP-China Telecom-v1.doc  Jun presents  JHU: depends on SA2 architecture  CT: can be in 6G study?  Tmo: is this part of SA2?  CT: yes, localized network is part of localized service delivery  E//: need to see SA2 work first before starting  DCM: also need to see SA2 result first |
| 8 | JHUAPL | WT-JHUAPL-v1.docx  Gino presents  DCM: should this be done in GSMA, like IR.67  JHU: part of the challenge is root of trust establishment, linkages to some future work, appropriate for SA3  Nokia: interdomain, GSMA is the right entity, for intradomain do profiling  JHU: IETF provides toolbox, specify how provide interoperator and intervendor interoperability |
| 9 | Charter | WT-Charter-v-1-0.docx  Achari presents  CATT: missing other SA2 work tasks  Charter: 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 here  Vivo: WT 2, third bullet is not interworking  Charter: 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 architecture  Nokia: what is secure migration, non 3GPP access also needs SA2 alignment  Charter: study will determine the details, interworking is well understood |
| 10 | Samsung | DP-Samsung-v01.doc,  WT-Samsung-v01.docx  Rohini presents  Nokia: concern on indepent WT on false base station, know certain gaps exist, consider this an independent WT  Samsung: want this under 6G umbrella SID  E//: 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 themselves  QC: 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 scope  Apple: generally support this proposal, agree with comment on SA1 requirements  Vivo: agree with Apple: WT4 and 1.2 overlap  DCM: could this be combined with the SA2 SID description  Chair: need to have this discussion in the actual SID discussion, want to give this  E//: what to do with RAN  Tmo: also do more general security work  ATT: set TUs aside to address 6G system security  Oppo: RAN groups discussion already raised MACce security considerations  Chair: preference is to have separate work tasks, assign TUs per work tasks  E//: 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 |