**Agenda:**

1) Secondary authentication for UE onboarding **(30 min)**

S3-220688          Clarifications to secondary authentication for UE onboarding        Intel Corporation (UK) Ltd

S3-220939          Corrections and clarifications to secondary authentication during UE onboarding   Ericsson

Added: S3-220687          Clarifications to secondary authentication PDU Session Container           Intel Corporation (UK) Ltd   (only the change between steps 10 and 11)

2) UE decision to send anonymous SUCI **(30 min)**

**For all contributions, focus on UE decision to send anonymous SUCI**

S3-220863          Address Ens for NPN       Huawei, HiSilicon (first change)

S3-220912          Definition of Anonymous SUCI   Ericsson, Qualcomm (second change)

S3-221002          Resolving Editor’s note on using only null-scheme SUCI              Qualcomm Incorporated (changes in step 1)

**From CT1 rapporteur** (Ivo Sedlacek, Ericsson)

The following CT1 CRs for eNPN WI submitted to ongoing CT1 meeting depend on SA3 decisions:

1) C1-223402 ("Anonymous SUCI usage") [1] and C1-223403 ("Configuration for anonymous SUCI usage") [2] - comments were raised in CT1 that a clarification in stage-2 is needed, to be clear based on what the UE determines to use anonymous SUCI. No formal dependency on SA3 CR.

NOTE: Dependency on TS 23.003 CR 0626 indicated in cover pages of C1-223402 ("Anonymous SUCI usage") [1] and C1-223403 ("Configuration for anonymous SUCI usage") [2] is an error as TS 23.003 CR 0626 has been approved in Mar 2022 CT plenary and is already part of 23.003 v17.5.0.

2) C1-223796 ("Onboarding SNPN and secondary authentication support") [3] is formally dependent on S3-220688 [5]. Comments were raised in CT1 that companies would like to see an agreed SA3 CR before agreeing CT1 CR.

3) C1-223799 ("SM PDU DN in case of SNPN onboarding") [4] is formally dependent on S3-220687 [6]. Comments were raised in CT1 that companies would like to see an agreed SA3 CR before agreeing CT1 CR.

[1] <https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_136e/Docs/C1-223402.zip>

[2] <https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_136e/Docs/C1-223403.zip>

[3] <https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_136e/Docs/C1-223796.zip>

[4] <https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_136e/Docs/C1-223799.zip>

[5] <https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_107e/Docs/S3-220688.zip>

[6] <https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_107e/Docs/S3-220687.zip>

**Notes**

**1) Secondary auth**

S3-220688, Intel presents.

S3-220939, Ericsson present

Intel: No interest in DN-AAA case, removing fine. Don't understand need for second set of credentials.

Ericsson: How can it be same set of credentials for different auth methods?

Intel: Use case for different auth methods?

Ericsson: Specification does allow, it was discussed and decided earlier.

Intel: UE does not know whether network will challenge for secondary authentication, only one of three architectures. Will all UEs be configured with default PDU session auth and authz credentials? Second type of credentials will never be used.

Ericsson: Default PDU session authentication and authz credentials could be left empty?

QC: Default UE credentials are for primary authentication. May optionally require credentials for secondary authentication. Special case where primary and secondary auth use same set of credentials. So primary and secondary credentials separate, but part of default UE credentials.

On DN-AAA case. UE will only respond with credentials if network asks.

Ericsson CT1: CT1 needs to know which credentials to use in primary and which in secondary authentication.

QC: UE implementation, but CT1 can differentiate. Primary credentials always for primary.

Ericsson CT1: Need different names to differentiate.

QC: SA2 defined default credentials.

Ericsson CT1: Default PDU session authentication and authorization credentials as part of default credentials then.

Intel: Default UE credentials for primary authentication.

QC: No, default UE credentials for primary and secondary.

Intel: How does UE know which to use?

QC: associated with SUPI / PDU session

Ericsson: Seems to be terminology. Proposal: "Default UE credentials used for primary authentication", "Default UE credentials used for secondary authentication".

QC: One way to solve the problem. Alternatively "Default UE credentials consist of credentials for primary authentication and optionally credentials for secondary authentication".

Intel: What if they are the same?

QC: Need to configure them to be the same.

Intel: Text that Ericsson proposed fine, if they can be the same.

QC: Not same for different purposes.

Ericsson: DN-AAA case needed or not.

QC: No strong opinion, but both cases allowed, not prevent.

Intel CT1: Which credentials?

QC: Two cases. Must have primary auth credentials. Secondary may require secondary auth credentials.

Ericsson CT1: Fallback to primary also in secondary auth would disclose to DCS.

Intel: TLS can use same credentials.

QC: Do not want to disclose UE IDs to DCS if primary and secondary use same credentials. E.g. if UE id is IMEI, do not want to disclose.

S3-220688, Intel presents (changes between steps 10 and 11)

Intel: secondary auth as part of UE onboarding: sending DN specific ID in step 4 (PDU session est req) not needed

Ericsson CT1: discussed in CT1, need normative req, not in SA2

QC: reasoning of change?

Intel: UE should not disclose. Difference between UE configured to use secondary auth.

QC: Do not see why need to make this separate. Need to configure credentials with secondary auth.

QC: Do not want to disclose credentials for primary to secondary authentication.

**2) Anonymous SUCI**

S3-220863, Huawei presents: Re-use MSK configuration for use of anonymous SUCI. Benefit that SNPN does not to take privacy responsibility.

S3-220912, Ericsson presents: ME generates the anonymous SUCI based on configuration. UE needs to know whether to use anonymous SUCI.

S3-221002, QC presents: Indication to use anonymous SUCI and use MSK need to be separate.

Ericsson CT1: Do not think that Huawei's approach works. Anonymous SUCI can be used towards AUSF (Annex B), then EMSK is used instead of MSK.

Huawei: Annex I and O are informative, so no implementation yet. Credentials stored on ME. QC and Ericsson solution does not work if storage on USIM. How does the ME know that the UE supports privacy? Additional indication between USIM and ME.

Ericsson CT1: Referred to Annex B. Annex I (normative) refers to Annex B.

QC: Agree that EAP-TLS can be used in two configurations, EMSK (Rel-15) and MSK.

Ericsson: There is also the case that EAP method does not support anonymous, but key hierarchy based on MSK.

Huawei: Annex B is informative. ME can have its own implementation.

QC: If same indication for two purposes (Privacy, key hierarchy), not possible to differentiate between different cases.

Huawei: Asks QC to clarify

QC: Legacy AAA (-> MSK) and SUPI privacy two different cases. No indication, only configuration.

Huawei: Your solution will not work for USIM. If credentials stored on USIM, ME will not know. Only for EAP framework.

QC: If non-AKA methods but credentials on USIM, need proprietary interface between ME and USIM to indicate. Need for MSK indication as well if credentials on USIM.

Huawei: Need to check. Can both AKA and non-AKA auth be used in CH case?

QC: Separate issue. With AKA need AUSF/UDM.

Thales: does not agree. EAP-AKA' with AAA shall not be precluded.

Ericsson CT1: Question is indication to use anonymous SUCI.

Nokia: Proposal to use null-scheme for not EAP-TLS not good for privacy, not acceptable. How to conceal and store public key out of scope. Why don't use existing methods.

QC: Misunderstood QC proposal. When legacy AAA architecture, privacy at the EAP layer. Other methods including EAP-TLS that implement privacy. If privacy, achieve at EAP layer.

Ericsson CT1: If null scheme used, which are the conditions to use anonymous SUCI?

Huawei: QC and Ericsson solution has problem if credentials stored on USIM, and indication on ME.

QC: Need to implement between USIM and ME vendor.

Huawei: How does ME vendor know?

Discussion about where credentials are stored and whether it's standardized.

Huawei: May need to look at CT1 specifications.

Thales: Disagree with assumption that non-AKA in ME.

Ericsson CT1: 23.122 stage-2 specification.

QC: will not get an agreement in SA3.

Ericsson CT1: UE does not know whether authentication by AUSF or CH, anonymous SUCI can be used against both, K\_AUSF depends on whether authentication by AUSF and CH.

Huawei: CH legacy AAA, shall use anonymous SUCI based on indication.

QC: Indication that privacy is needed.

Lenovo: Cannot accept selective privacy solution that only works for selective EAP methods.