**3GPP TSG-SA3 Meeting #115AdHoc-e S3-241438-r1**

**Electronic meeting, online, 15 - 19 April 2024**

**Source: Ericsson**

**Title: Clarifications for privacy options in EAP-TLS**

**Document for: Approval**

**Agenda Item: 4.8**

# 1 Decision/action requested

***This document proposes to add clarifications to the Annex B of the living document [1] to clarify the changes regarding privacy in EAP-TLS 1.2 and 1.3.***

# 2 References

[1] S3-241108 Living document for CryptoSP: draftCR to TS 33.501, Updates to cryptographic profiles

[2] 3GPP TS 33.501 Security architecture and procedures for 5G system

# 3 Rationale

## 3.1 Background

Privacy considerations for EAP-TLS are described in Annex B.2.1.2 of TS 33-501 [2]. The intention of that clause is to describe how the two privacy mechanisms work together i.e. privacy in NAS layer (SUCI scheme) and privacy in TLS layer.

Clause B.2.1.2.1 describes the case when EAP-TLS does not provide any privacy. This is only relevant for EAP-TLS 1.2 (**case 1**).

Clause B.2.1.2.2 describes the case when EAP-TLS does provide privacy. This is either EAP-TLS 1.3 or EAP-TLS 1.2 with privacy option activated (**case 2**).

Currently the last paragraph of clause B.2.1.2.1 relates to **case 2**, so this document proposes to move that paragraph to clause B.2.1.2.2 and clarify that is only applicable for EAP-TLS 1.2 (with privacy option).

Further, this document proposes to add a paragraph in clause B.2.1.2.2 that explains that EAP-TLS 1.3 forbids the sending of username in cleartext in the identity response or any message used instead of the identity response. Hence EAP-TLS 1.3 forbids the use of "null-scheme" for SUPI privacy in NAS layer, unless an anonymous identifier is used.

## 3.2 Reason for change

Current description of privacy options in Annex B.2.1.2 is not fully correct. For EAP-TLS 1.3 it is not allowed to send plaintext SUPI (except in case of anonymous SUCI). Clarifications are needed regarding how privacy in NAS layer and privacy in EAP-TLS 1.2 can be used.

## 3.3 Summary of change

Adding a new sub clause in Annex B.2.1.2 with general information. Moving one paragraph from B.2.1.2.1 to B.2.1.2.2. Adding text in B.2.1.2.2 describing that for EAP-TLS 1.3 it is not allowed to send plaintext SUPI.

## 3.4 Affected clasues

Appendix B.2.1.2.

# 4 Detailed proposal

## \*\*\*\*\*\* START OF CHANGES **\*\*\*\***

### B.2.1.2 Privacy considerations

#### B.2.1.2.0 General

This clause contains considerations about usage of privacy in the NAS layer, i.e. SUCI privacy as described in clause 6.12, together with privacy in the EAP-TLS layer. Annex B.2.1.2.1 describes the case when EAP-TLS does not provide any privacy, which is only relevant for EAP-TLS 1.2. Annex B.2.1.2.2 describes the case when EAP-TLS does provide privacy, i.e. either EAP-TLS 1.3 or EAP-TLS 1.2 with privacy option activated.

#### B.2.1.2.1 EAP-TLS without subscription identifier privacy (EAP-TLS 1.2 only)

For EAP TLS 1.2, if the operator determines to not provide subscription identifier privacy for the UE in EAP-TLS layer (in EAP-TLS 1.2 without privacy option), the subscription identifier protection in NAS layer, i.e., in Step 1 of Figure B.2.1-1, becomes ineffective privacy-wise. Therefore, the operator may just choose that UE uses "null-scheme" for calculation of SUCI which is sent in NAS layer. However, the operator may anyway use other than null-schemes (e.g., one of ECIES schemes) for simplification of having single scheme for all UEs in NAS layer even though privacy is not enhanced in this particular case.

####

#### B.2.1.2.2 EAP-TLS with subscription identifier privacy

For EAP-TLS, if the operator determines to provide subscription identifier privacy for the UE in TLS layer, the EAP-TLS server needs to support privacy either inherently (as in EAP-TLS 1.3) or via separate privacy option (as in EAP-TLS 1.2). If privacy is an option in EAP-TLS layer (i.e. EAP-TLS 1.2), then the operator needs to configure UE with the information that privacy-on-TLS layer is enabled. For EAP-TLS 1.3, privacy is mandatory and thus needs no configuration. Further, the following considerations need to be taken.

If the UE is configured to use privacy option in EAP-TLS 1.2, the operator could still determine not to provide subscription identifier privacy for the UE in NAS layer. In such case, the operator may just choose that UE uses "null-scheme" for calculation of SUCI which is sent in NAS layer. In this case the privacy in the EAP-TLS layer becomes ineffective privacy-wise.

EAP-TLS 1.3 [76] inherently provides privacy. Section 2.1.8 of EAP-TLS [76] states:

"A client supporting TLS 1.3 MUST NOT send its username (or any other permanent identifiers) in cleartext in the Identity Response (or any message used instead of the Identity Response)."

Hence, null- scheme SUCI cannot be used for EAP-TLS 1.3, unless an anonymous identifier is used (see below).

In Step 1 of Figure B.2.1-1 and Figure B.2.1-2, it is important that calculation of SUCI, which is sent in NAS layer, is done using schemes other than "null-scheme". Otherwise, the subscription identifier protection provided by EAP-TLS layer becomes ineffective privacy-wise. Nevertheless, the “null-scheme” could be used in NAS layer while still preserving subscription identifier privacy, by omitting the username part from NAI as described in RFC 4282 clause 2.3 [y]. It would be analogous to using anonymous identifier in EAP, meaning that only realm part from NAI is included in SUCI which is sent in NAS layer. Thus formed SUCI can still be used to route the authentication request to AUSF.

In Step 13 and 14 of Figure B.2.1-1, when EAP-TLS 1.2 is used, the UE would need to behave as described in "Section 2.1.4. Privacy" of RFC 5216 [38] where instead of sending the client certificate in cleartext over the air, the UE first sends TLS certificate (no cert) and only later sends TLS certificate after a TLS connection is setup.

## \*\*\*\*\*\* END OF CHANGES **\*\*\*\***