**SA3#104-e: offline conf call on FS\_eNPN\_SEC**

**EAP-TTLS**

|  |  |  |
| --- | --- | --- |
| [**S3-212521**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212521.zip) | Further conclusions for KI #1 | CableLabs,Ericsson, Charter Communications, Intel |

**MSK indication**

|  |  |  |
| --- | --- | --- |
| [**S3-212700**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212700.zip) | Conclusion on KI#1 for key derivation | Huawei, HiSilicon |

|  |  |  |
| --- | --- | --- |
| [**S3-212868**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212868.zip) | pCR: Additional conclusions for KI #1 | Qualcomm Incorporated |

**EAP-TTLS**

CableLabs: r1 and r2 available

Nokia: Agree to EAP-TTLS in general. Question is about protection of key material. Compromise was agreed in SA2. However, this situation is different. Now TTLS server is moved into NSSAAF, with key material and all exposed to external interfaces, this is going too far. Do not want to expose key material to outside the network. And do not want another intermediate function.

Ericsson: what exactly is the issue with r2?

Nokia: The issue is the word "possible", guessing about discussions in normative phase.

Ericsson: If the sentence "possible colocation … " is removed?

Nokia: No, because it still mentions AAA-H. Need more time to evaluate this new function.

Ericsson: Wonder how discussion would go next week when discussing procedures. Is it realistic to agree next week?

Nokia: Worth a try.

Huawei: Could extend to next week.

Ericsson: Or we could discuss directly when discussing text for informative annex.

CableLabs: Suggestion to agree on r1, close this document, discuss rest in next week.

Ericsson: Could live with that.

**MSK indication**

Huawei: presents 2700. AMF indicates usage of MSK with ABBA.

Ericsson (rapp): 2868-r1 proposes indication at UE

Ericsson: Earlier we proposed indication by network, but requires AMF to be updated. So need to use indication at UE as baseline.

Huawei: Indication at UE does not work in onboarding scenario. Indication is per credential, so indication should be bound to credential. Not supported by UP protocol.

Ericsson: none of the existing provisioning protocols like CMPv2 works out of the box for 3GPP, would need 3GPP specific additions anyway

Huawei: when is the indication provisioned?

Ericsson: when credentials are provisioned

Huawei: ME will configure indication together with credentials. Would not work together with EAP-TLS. How would the ME distinguish?

Ericsson: per credentials, not per authentication method

Huawei: then CMPv2 would need to be updated

Ericsson: could be by 3GPP specific addition

Huawei: want to capture in evaluation part. For this meeting, focus on evaluation, can conclude at next meeting. No need to rush.

Ericsson: yes, that would be the consequence, start normative work this meeting, add MSK indication next time.

CableLabs: asks chair to extend time to second meeting week? Also, issue that indication is tied to credentials? Indication should be on the network side. But using ABBA also has issues.

Ericsson: try to avoid extending to next week

Huawei: if we focus on certificate on the UE, may be used for internal EAP-TLS and also external EAP-TLS.

CableLabs: also believe there could be issues. If user provides credentials?

Huawei: try to extend discussion to next week.

Ericsson: Suresh, is that possible?

Chair: agenda for next week is overloaded already. Could present later today at plenary.

Ericsson: That would be good.

Chair: can we try to come to an agreement today?

CableLabs: try to find an agreement

Ericsson (rapp): Discuss at official call today, see whether we can resolve, otherwise see whether need to be extended to next week.

Ericsson (HV): Encourage to bring your views today.

Nokia: discuss KI#4?

**KI#4**

Nokia: discussion has been mutual vs one-way authentication. Do not want to complicate solution for deployment. Want to make it optional for O-SNPN to have connection to DCS. This would be lightweight, but still provide mutual authentication.

Ericsson: This would mean usual primary authentication as already specified.

Nokia: Want to have the interface to DCS optional. Also want to describe mutual authentication in context of initial access.

Huawei: So AUSF will have been provisioned with certificate?

Nokia: Yes. But PKI out of scope.

Huawei: As EAP-TLS in current TS 33.501?

Nokia: Reference to EAP-TLS and make interface to DCS optional.

Ericsson: Do not quite understand why it is necessary. But can send concrete proposal for conclusion.