* API invoker authentication problem in current onboarding procedure

1. According to TS 33.122, API invokers need to complete the certificate-based mutual authentication on CAPIF-1e interface before being configured with the authentication methods related to AEF.

2. According to clause 8.10.3 of TS 23.222, API invokers need to do the onboarding procedure before obtaining the certificate used in CAPIF-1e.

3. According to clause 6.1 of TS 33.222, API invokers leverage the onboarding credential (i.e. OAuth 2.0 access token) to request the onboarding. The access token is about authorization rather than authentication.

4. There is no API invoker authentication in the current onboarding procedure. Malicious API invokers may impersonate legal invokers to do the onboarding.

* Potential requirements in KI #1

1. API invoker in KI #1 is a part of CAPIF and should do the onboarding procedure.

2. Should we add a requirement like “API invokers should be authentication before triggering the onboarding procedure” in KI #1?

E//: as there is no identifier, the authentication doesn't work.

Xiaomi: when access token is used, if no authentication is used, the API invoker may be impersonated by malicious invoker, so do we need a requirement, or do we just ignore it

Huawei: is this issue triggered by SNAAPPY or existing.

Xiaomi: CAPIF problem, but can be done under SNAAPPY

Huawei: TEI plus CAPIF should be the place for that.

Xiaomi: CAPIF is not solid here.

Huawei: this is enhancement of current CAPIF, no SNAAPPY specific issue.

DCM: without identifier scheme for invokers, not clear how to progress with authentication at all.

Xiaomi: progress on current CAPIF structure, or add a new onboarding mechanism?

DCM: only stable identifier is SUPI, but because SNAAPPY is on application layer, this probably won't help, proposal: rely on CAPIF structure, unless SA1 has a clear use case in which SUPI is a useful identifier.

Xiaomi: UE has more identifiers: AKID, also can be used on application layer., from AKMA, also BTID from GBA. Also GPSI

DCM: problem with authenticating application

Xiaomi: typically relies on certificate

E//: onboarding relies on authentication, some solutions may rely on onboarding, so no specific requirements required.