**KI2. A&A between EEC-ECS**

**Authentication:**

- Server(ECS) side certificate authentication (mandatory)+ Application layer (e.g. OpenID) for EEC side authentication (mandatory)

Supporting: Ericsson, Intel, Huawei

Not supporting:

E///: could be extended to token based authentication.

Thales: not supporting the only option for the conclusion.

Docomo: would like to make sure the necessity on the EEC side authentication.

- Server(ECS) side certificate authentication (mandatory)+ Application layer for EEC side authentication (Optional)

Supporting: Docomo, Huawei

E///: needs to check SA6.

- AKMA, TLS

Supporting: QC, Huawei, CMCC, Samsung/Lenovo/ZTE (non-roaming case)

Not supporting: Apple

- AKMA with key isolation:

Supporting: Apple.

Not Supporting: Ericsson, Huawei, QC

Ericsson: the solution can not be used for EEC authentication.

Huawei: should be addressed in the AKMA topic.

- GBA, TLS

Supporting: Thale, QC, Huawei

Not supporting:

Ericsson: the solution can not be used for EEC authentication.

QC: GBA can work from 4G to 5G.

- Kamf based solution for roaming:

Supporting: Samsung, Lenovo, ZTE

Not supporting: CMCC, QC, Huawei, Ericsson

- Certificate based on GSMA Spec

Supporting: Thales

Not supporting: QC, Ericsson

**Authorization:**

-static authorization: 2644 (Huawei),

**KI1. A&A between EEC-EES**

**Authentication:**

- Server side authentication+ Application layer (e.g. OpenID)

Supporting: Ericsson, Samsung, Intel, Huawei

No supporting:

- AKMA, TLS

Supporting: QC, Huawei, CMCC

Not supporting: Samsung, Lenovo, Apple

- AKMA with key isolation:

Supporting: Apple.

Not Supporting: Ericsson, Huawei, QC

- GBA, TLS

Supporting: Thale, QC, Huawei

No supporting:

- Kamf based solution for roaming:

Supporting: Samsung, Lenovo, ZTE

No supporting: CMCC, QC, Huawei, Ericsson

- Certificate based on GSMA Spec

Supporting: Thale

No supporting: QC, Ericsson

**Authorization:**

-Token generated by ECS: 2643(Huawei), 3010 (Thales),

-Static authorization: 2643(Huawei),