**SA3 teleconference for Edge computing security**

**20210806**

**Active participants: Samsung, Thales, Qualcomm, Ericsson, Lenovo, Apple, ZTE, TelecomItalia, Huawei**

# Key issue #1

## S3-21xxxx-EDGE-conclusion-KI1

Authentication and authorization between EEC and EES:

* Solution #3 and Solution#17 is recommended as the baseline for the normative work to conclude that EEC and the EES establish a secure TLS connection using EES (server-side) certificate. For authentication of EEC, access token by OAuth is used. TLS provides integrity protection, replay protection, and confidentiality protection over the EDGE-1 interface. EEC produces the access token to the EES, over the EDGE-1 interface securely.

**E//:** reformulation is required. Three entities. ECS can authenticate the EEC, and generate the token. Token can be used for authentication or maybe authorization.

**Huawei:** whether the token is used for both authentication and authorization.

**Samsung:** same token for the A&A.

**Thales:** Thales has solution 27, which would be the othe choice for the authentication.

**E//:** EN on clarification should be solved at first.

**Thales:** GSMA specification is referred. Edge security service and its API is defiend by GSMA. New SIM card is required.

* Authorization of the EEC is based on the access token generated by the ECS for the EES service which is described in solution #3 and #17. It is recommended to use solution #3 and solution#17 as the baseline for the normative work.

## S3-21xxxx-2\_conclusion on KI1\_was\_draft\_S3-211893-r5 (2)

### 7.1 Conclusions for Key Issue #1

It is concluded are as follows:

Authentication issue between EEC and EES:

* AKMA based authentication and data protection.
	+ Solution #16, and #24are recommended as the baseline for the normative work to include that AKMA is used for generating the shared key between EEC and EES, and TLS is used to authenticate with each other based on the shared key. The version for appling AKMA with TLS is left for the normative work.

**QC**: CR is approved. Reuse the standardized method on the TLS based on AKMA. Slightly difference with #24.

* GBA based authentication and data protection
	+ Solution #29 is recommended as the baseline for the normative work to include the GBA based TLS mutual authentication between EEC and EES.
* Certificate based mutual authentication and data protection
	+ Solution #4, and #17 are recommended as the baseline for the normative work to include the certificate based TLS mutual authentication between EEC and EES.

NOTE 1: Certificate allocation for the EEC is out of scope of the present document.

**Thales:** #27 has the solution on providing certificates to the EEC. Certificate based mutual authentication can be supported.

**QC:** certificate could be an alternative solution if out of band can be used. People can pick an easy solution on TLS based on the certificate provision if they would like to use.

* Kamf based authentication and data protection
	+ Solution #7 are recommended as the baseline for the normative work to include mutual authentication between EEC and EES.

**E//:** big impact on the authentication. It may need a new SID to study this. There is a AKMA solution supporting this type of solution. May not a good choice to define this new feature.

**Lenovo:** see the evaluation, no big impact with other solutions.

**Huawei:** similar comments with E///. It is a whole new mechanism, which needs to be discussed.

**QC:** similar with E///.

**Samsung:** support this as an alternative as AKMA. Beneficial to use Kamf for the edge sevices.

**ZTE:** support this solution. Roaming is not considering in AKMA. Solution is benefit for the roaming case.

**Huawei:** roaming is not an issue for AKMA. AKMA can be easily updated with proxy to support roaming.

**Lenovo:** no see how to enhance the AKMA with the roaming.

- EES authentication using TLS based the server’s certificate + EEC authentication with the token generated by the ECS

* + Solution #17 are recommended as the baseline for the normative work to include the certificate based TLS mutual authentication between EEC and EES.

NOTE 1: Regarding that EEC ID generation is out of scope of TS 23.558 [2], EEC ID verification is out of the scope of the present documents as well.

**E///:** EEC ID

**Apple:** we can take the EEC ID as authenticated if it is not verified.

**E//:** if there is no EEC ID, AKMA and GBA only verify the UE ID. Key issue required that EEC is authenticated.

**QC:** people may not care about the application ID (eeC ID) verification if authentication could be provided by the UE.

**Samsung:** EEC ID is unique. SA6, EEC ID may no unique. Devices may the same EEC ID. If it is not unequal, we have to revisit the key issue. Provide the reference via the SA3 reflector.

## S3-21yyyy-EDGE-conclusion-KI2 (2)

## 7.x Conclusion for Key Issue #2

Authentication between EEC and ECS:

* Solution #3 is recommended as the baseline for the normative work to conclude that AKMA is used for generating the shared key between EEC and ECS and TLS-PSK protocol is used for mutual authentication.
* In case of roaming, as to have support of EDGE service provided in the serving network, it is recommended to use solution#7 as the baseline for normative work for Rel-17, in addition to Solution #3.
	+ Currently, AKMA does not support roaming scenarios in Rel-17. Therefore, it is practically impossible for all external AFs (in the roaming networks) to have **secure** N33 interface with the NEF (in the HN of the roaming UE).
	+ Solution#7 to be considered as an interim solution, until AKMA supports roaming scenarios.

**Lenovo:** support.

**Thales:** we have the gba based solution #29. And #27 solution for the authentication..

**QC:** not agree to use #3 on the authentication.

## S3-21yyyy-2\_conclusion on KI2\_was\_\_S3-211894-r4 (2)

### 7.2 Conclusions for Key Issue #2

It is concluded are as follows:

Authentication issue between EEC and ECS:

* AKMA based authentication and data protection.
	+ Solution #3, and #24 #28 are recommended for the normative work to include that AKMA is used for generating the shared key between EEC and ECS, and TLS is used to authenticate with each other based on the shared key. The version for appling AKMA with TLS is left for the normative work.

**Apple:** #28 uses Kamka + EEC ID as the key genenration. It supported to authentication the EEC ID as well. (key issue #2). Key isolation provided by #28. EEC ID authentication is not related with this solution.

Authorization issue between EEC and ECS

* Using the static authorization by the ECS for the ECS service authorization.
* ECSP generates token for the EEC. EEC forwards the token to the ECS for authorization.

**Huawei:** not sure whether we could define the ECSP in SA3.

**E//:** security mechasim of ECSP can be defined in SA3. Even it is not defined by SA6.

## S3-21zzzz-3GPP\_TS 33.558 skeleton

**TelecomItalia:** the specific architecture should be added. Currently, there is a place to clarify the architecture. There may be a large number of architectures.

**Huawei:** will consider your suggestion in the skeleton.