**3GPP TSG-SA3 Meeting #118 S3-242xxx**

Hyderabad, India 14 - 18 October 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title: Evaluation summary of solutions for KI#2.1**

**Document for: Approval**

**Agenda Item: 5.14**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

<Examples of references, please delete when you have inserted your actual references:

[1]

# 3 Rationale

*(With bullet points, describe the reasons for the proposed action.
The objectives of the proposal should be clearly stated.
Rejected alternative solutions should be mentioned if this aids understanding).*

*(For pseudo CR, the reason for change(s) and summary of change(s) must be clearly explained.)*

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*START of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

## 7.2 Evaluation summary of the solutions for KI#2.1

The following table 7.2-1 shows concisely how the threats and security requirements of KI#2.1 have been addressed by the different solutions in clause 6 of the present document.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Threat #1| Req. #1 (clauses 5.3.1.2.1 & 5.3.1.3.1) | Threat #2 | Req. #2(clauses 5.3.1.2.2 & 5.3.1.3.2) | Impact / Observations |
| Solution #1 (Clause 6.1) | User information provided by the EEC is private IP addressThe solution verifies the provided IP address (private) by querying the UPF NAT mapping table. | It is not addressed.It uses both private and public IP address of the UE. | It requires NAT functionality to be embedded in UPF.It leverages the mapping between public and private IP to verify the provided (private) IP. It exposes the private and public IP addresses of EEC to EES. EES can be inside or outside the operator domain.  |
| Solution #2(Clause 6.2) | User information provided by the EEC is a hash value computed by using private information (e.g., SUPI) + counter.Nnef\_UEId API is invoked with hash value and UE IP address. The hash is used to verify the IP address provided by AF to NEF in the invocation. | It is not addressed.It uses private IP address of the UE to invoke 5GC API, that can be used to break the user privacy. | AF needs to be able to reach UE (AF initiates the communication in step 1) to trigger the hash generation. The data used for generating the hash determines the strength of the verification. The hash can be subject to brute-force type of attacks. It prevents replay attacks from malicious AF, since the hash is different in every API invocation.  |
| Solution #3(Clause 6.3) | User information provided by the EEC is a temporary ID, generated and provided by the 5GC for PDU session. The 5GC verifies the temporary ID provided by the AF with the one generated for the UE.  | The user information provided by the EEC is a temporary ID assigned by the Core, thus the privacy of the UE is preserved.  | The UE needs to request the temporary ID in the PDU session establishment/modification request and provide it to the EEC.It does not require to expose any network information outside the 5GC, such as to EDGE servers. |
| Solution #4(Clause 6.4) | User information provided by the EEC is A-KID coming from AKMA procedure.AKMA guarantees that the information provided is trusted.  | 5G UE Id is not required to fetched as per authentication service provided by AKMA. The privacy of the UE is implicitly preserved.  | The solution requires AKMA to be implemented from the operatorIt does not require to expose any network information outside the 5GC to EDGE servers |
| Solution #5(Clause 6.5) | EEC provides a signed version of the required data, i.e., private IP address, along with a certificate to prove their authenticity. | It is not addressed.Signature only provides integrity protection but does not provide confidentiality of the information, therefore the EES can still collect the IP address | It requires an additional CA system for the EEC (UE) trusted by all EES, or other schemas like cross-certification are to be considered. It requires that the certificate includes also the IP address. |
| Solution #6(Clause 6.6) | The EEC provides a token-based solution that directly allows EES to retrieve the corresponding 5G UE ID.UE ID server ensures the authenticity of the token. | The user information provided by the EEC is a Token that does not contain privacy concerning information, thus the privacy of the UE is preserved.  | The solution introduces a new Networn Element (UE ID Server)It does not require to expose any network information outside the 5GC to EDGE servers. |
| Solution #7(Clause 6.7) | The EEC provides the PDU session ID along with the IP address, the NEF uses the IP address to retrieve the PDU session ID from UDM and compare it with the one received from EES | It is not addressed.The private IP address is still provided along with the PDU session ID. | The UE privacy protection relies on the usage of the PDU session ID. In particular, it is required to understand whether the PDU session ID is a sensible information and whether brute-force attacks are possible on it.  |
| Solution #8(Clause 6.8) | The EEC provides IP address and access token (OAuth), which includes UE ID (??) Access token is used for the verification of the IP address.  | It is not addressedThe private IP address is sent along with the access token | Comment: ENs need to be resolved. |