**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230021-r2***

**Electronic meeting, 16 - 20 January 2023**

**Source: BSI, Nokia, Nokia Shanghai Bell**

**Title: KI10 solution 25 update on security profiles**

**Document for: Approval, Information, Discussion**

**Agenda Item: 5.24**

# 1 Decision/action requested

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

# 2 References

[1] TR 33.875

# 3 Rationale

*Proposes to replace “null” PRINS with “integrity-only” PRINS, as this more accurately reflects the solution.*

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

1st CHANGE

### 6.25.2 Solution details

To facilitate and simplify the deployment and operation of PRINS as one N32 security solution, it is proposed to introduce security profiles.

N32-c negotiation for PRINS is enhanced to allow selecting the existing scheme (for backward compatibility and high security requirements voiced in discussions) or selecting one or several security profiles.

* Only by selecting "full PRINS“, negotiation of a cipher suite and exchange of modification and encryption policies is needed (current schema).
* If a pre-defined profile, e.g. "profile A" or "profile B", is chosen, a pre-defined security profile will be negotiated between SEPPs, and IPX can be instructed equally.
* "integrity-only PRINS" could be then one option, which in current understanding means, that JSON objects are created without encryption policies but integrity protected. NOTE: integrity-only PRINS may however not be preferable, since AVs and authorization tokens need protection

With this information, during N32-c handshake, if the PRINS enhanced profile, e.g., “B”, is chosen, then both SEPPs (VPLMN and HPLMN) know how to handle the communication on the N32-f interface and the intermediary IPX providers as well. I.e., a profile indicator during N32-c negotiation phase can be propagated as an indication of the selected PRINS profile to the IPX; since only PRINS can be chosen, N32-f will always be based on application layer.

|  |  |
| --- | --- |
| Enumaration value | Description |
| TLS | TLS security |
| PRINS* Profile full
* Profile integrity-only
* Profile A
* Profile B
* …
* Operator defined profile
 | Protocol for N32 Interconnect security with subcategories to indicate full usage of PRINS, with integrity protection onl or specific profiles  |

Figure 6.X.2-1: Example of N32 security profile

If PRINS with "full PRINS" is chosen, configuration parameters can still be negotiated/exchanged, which keeps market open to those, really wanting this high security option

a. Modification policy. A modification policy indicates which IEs can be modified by an IPX provider of the sending SEPP.

b. Data-type encryption policy. A data-type encryption policy indicates which types of data will be encrypted by the sending SEPP.

c. Cipher suites for confidentiality and integrity protection, when application layer security is used to protect HTTP messages between them.

d. N32-f context ID. The N32-f context ID identifies the set of security related configuration parameters applicable to a protected message received from a SEPP in a different PLMN.

If PRINS with any other profile is chosen, the following configuration parameters need to be negotiated/exchanged and profiles need to be defined.

1. A PRINS profile indicating a predefined set of one or more of the above policies.

NOTE: Data type encryption policy for integrity-only PRINS profile: this policy will not specify any data type to be confidentiality protected; Modification policy for integrity-only PRINS profile: this policy will specify any IE subject to be modifiable. Still, integrity protection is provided.

\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES