**3GPP TSG-SA3 Meeting #115 *draft\_S3-240889-r1***

**Athens, Greece, 26 February – 1 March November 2024**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Security profiles for PRINS |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | Roaming5G |  | ***Date:*** | 2024-03-01 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | The LS exchanges among 3GPP and GSMA show that the acceptance of an e2e security protocol in roaming is also dependent on easy handling of the PRINS protocol. See LS [**S3-240213**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_115_Athens/Docs/S3-240213.zip)PRINS allows an operator to selectively enable for a roaming intermediary what can be seen or modified at hops. To allow easier handling of the high number of IEs and the related MNO policy, GSMA NG.132 provides already details on the introduction of profiles and requested 3GPP again per LS to allow for the simplification of PRINS as it will be specified in detail in GSMA.  |
|  |  |
| ***Summary of change:*** | Reference to security profiles for PRINS for easier handling of modification policies for roaming intermediaries on the path. |
|  |  |
| ***Consequences if not approved:*** | Not allowing for a flexible use by different stakeholders in the roaming eco-system, when PRINS is selected as security mechanism. |
|  |  |
| ***Clauses affected:*** | 13.5 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | ***234865*** |

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

## 13.5 Security capability negotiation between SEPPs

The security capability negotiation over N32-c allows the SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32-f. There shall be an agreed security mechanism between a pair of SEPPs before conveying NF service-related signalling over N32-f.

When a SEPP notices that it does not have an agreed security mechanism for N32-f protection with a peer SEPP or if the security capabilities of the SEPP have been updated, the SEPP shall perform security capability negotiation with the peer SEPP over N32-c in order to determine, which security mechanism to use for protecting NF service-related signalling over N32-f. Certificate based authentication shall follow the profiles given in 3GPP TS 33.210 [3], clause 6.2.

A mutually authenticated TLS connection as defined in clause 13.1 shall be used for protecting security capability negotiation over N32-c. The TLS connection shall provide integrity, confidentiality and replay protection.



Figure 13.5-1 Security capability negotiation

1. The SEPP which initiated the TLS connection shall issue a POST request to the exchange-capability resource of the responding SEPP including the initiating SEPP’s supported security mechanisms for protecting the NF service-related signalling over N32-f (see Table 13.5-1). The security mechanisms shall be ordered in the initiating SEPP’s priority order.

2. The responding SEPP shall compare the received security capabilities to its own supported security capabilities and selects, based on its local policy (e.g. based on whether there are IPX providers on the path between the SEPPs), a security mechanism, which is supported by both initiating SEPP and responding SEPP.

3. The responding SEPP shall respond to the initiating SEPP with the selected security mechanism for protecting the NF service-related signalling over N32.

Table 13.5-1: NF service-related signalling traffic protection mechanisms over N32

|  |  |
| --- | --- |
| N32-f protection mechanism | Description |
| Mechanism 1 | PRINS (described in clause 13.2)  |
| Mechanism 2 | TLS |
| Mechanism n | Reserved |

If the selected security mechanism is PRINS, the SEPPs shall behave as specified in clause 13.2.

If the selected security mechanism is PRINS, the SEPP may indicate a security profile.

NOTE: can for example PRINS security profile specification is out of scope in 3GPP.

If the selected security mechanism is TLS, the SEPPs shall behave as specified in clause 13.1.2, tear down the N32-c connection and forward the NF service-related signalling over N32-f using a TLS connection.

If the selected security mechanism is a mechanism other than the ones specified in Table 13.5-1, the two SEPPs shall terminate the N32-c TLS connection.

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