**3GPP TSG-SA3 Meeting #123 S3-252589-r3**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: CableLabs, Nokia, Charter Communications, China Telecom, Deutsche Telekom, Comcast Communications, Verizon, CMCC, BSI**

**Title: New WID on PRINS Refinement**

**Document for: Approval**

**Agenda Item: 6.2**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: New WID on PRINS Refinement

Acronym: RefinePRINS

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-20 (5GA)

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | X |  |
| No | X | X | X |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Study  |
|  | Normative – Stage 1 |
| X | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  N/A |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| N/A |   |   |

# 3 Justification

GSMA NRG sent an LS (S3-252539) to 3GPP SA3 on further refinement of PRINS to make it easier for roaming intermediaries (RIs) to support PRINS and its end-to-end application layer security property. The following aspects of PRINS are identified for further refinement:

1. Using the HTTP CONNECT mechanism for the establishment of an end-to-end N32-c connection poses certain security risks for RIs. In particular, the HTTP CONNECT request, as currently specified, is not authenticated. As a result of this, unauthorised parties could impersonate a legitimate contractual partner of the RI and use this request for the establishment of connections without any contractual basis, for example, to send malicious traffic. In order to mitigate this risk, the RI should be able to make a decision on HTTP CONNECT requests based on an authenticated identity.

2. Information such as the protection policy exchanged between vSEPP and hSEPP via N32-c handshaking procedures [29.573] should be visible to RIs. N32-c, as currently specified, provides confidentiality between vSEPP and hSEPP, preventing the RIs in between from seeing the protection policy that is being exchanged between vSEPP and hSEPP. However, to make sure that the exchanged protection policy complies with the business contracts of the RIs, as well as assuring that it is consistent with the policy that might be configured in an RI, the protection policy should be visible to the RIs. Knowing the protection policy exchanged between vSEPP and hSEPP over N32-c can also help troubleshooting and improve RI’s confidence that its modification of N32-f information elements using PRINS will not be rejected by vSEPP or hSEPP. If security profiles, instead of protection policy, are exchanged, these profiles should be visible to RIs.

3. Currently, 3GPP TS 33.501 (clause 13.2.1 of TS 33.501) specifies two options for N32-f transport layer protection: NDS/IP and TLS VPN. However, in the case of TLS VPN, certificate authentication and validations are not clearly specified for RIs. Further clarification on certificate authentication and validation for N32-f transport layer protection would be beneficial to RIs.

We believe the refinements of PRINS requested by GSMA are reasonable and have the potential to enhance its deployability while maintaining its end-to-end security properties. Accordingly, we propose this work item to implement the proposed refinements of PRINS.

# 4 Objective

Based on the above justifications, the following objectives are proposed:

1. Protecting HTTP CONNECT requests and response by adding ,integrity protection and anti-replay protection . This allows an RI to cryptographically authenticate HTTP CONNECT requests and responses.

2. Allowing some parameters exchanged in N32-c procedures (e.g., protection policy) that are relevant to RIs to be made available to Ris..

3. Adding HTTPS as an option for protecting the transport of N32-f, in addition to NDS/IP domain security and TLS VPN.

## TU estimates

Total TU estimates: 2 TUs (4 meeting cycles)

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| 33.501 | Security architecture and procedures for 5G system | TSG#111(Mar 2026) |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

None

# 9 Supporting Individual Members

{At least 4 supporting Individual Members are needed. There is an expectation that these companies will provide resources to progress the work. Note that having 4 supporting companies is a necessary but not sufficient condition: the usual TSG approval process by consensus is needed for the WID approval}

|  |
| --- |
| Supporting IM name |
| CableLabs |
| China Telecom |
| Deutsche Telekom |
| Charter Communications |
| Comcast Communications |
| Nokia |
| Verizon |
| CMCC |
| BSI |