**3GPP TSG-SA3 Meeting #104-e *S3-214311-r2***

**16 – 27 August 2021, Online**

**Source: CableLabs**

**Title: New KI for Authentication of PLMNs over Roaming Hub**

**Document for: Approval**

**Agenda Item: 5.17**

# 1 Decision/action requested

***It is requested to approve the pCR.***

# 2 References

|  |  |
| --- | --- |
| [1] | 3GPP TR 33.875, “Study on enhanced security aspects of the 5G Service Based Architecture (SBA)”.  |

# 3 Rationale

When two PLMNs establish a roaming relationship via an interconnect provider (e.g., IPX), the TLS connections between the two PLMNs for N32-c interface will also be terminated at the interconnect provider, e.g., when DNS is used to intercept application layer traffic. Therefore, the two PLMNs cannot authenticate each other mutually based on the TLS layer as required by PRINS. As a result, the crypto context negotiated over N32-c does not provide protection required for N32-f.

Therefore, further study is required on how to support mutual authentication of PLMNs over an interconnect provider.

# 4 Detailed proposal

## 5.X Key issue #X: Authentication of PLMNs over Interconnect Provider

### 5.4.1 Key issue details

This key issue is about how to perform mutual authentication of PLMNs when roaming over one or more interconnect providers.

When two PLMNs establish a roaming relationship via an interconnect provider (e.g., IPX), the TLS connections between the two PLMNs for N32-c interface will also be terminated at the interconnect provider, e.g., when DNS is used to intercept application layer traffic. Therefore, the two PLMNs cannot authenticate each other mutually based on the TLS layer as required by PRINS. As a result, the crypto context negotiated over N32-c does not provide protection required for N32-f.

Therefore, further study is required on how to support mutual authentication of PLMNs over an interconnect provider.

### 5.4.2 Security threats

If two PLMNs cannot mutually authenticate each other during roaming over an interconnect provider, security protection negotiated between the two PLMNs over N32-c cannot be trusted, resulting in security threats such as roaming fraud.

### 5.4.3 Potential security requirements

TBD