LIAISON STATEMENT

Title: **Comments from ETSI TC CYBER on GSMA Solutions for Monitoring of Encrypted 5GS Signaling Traffic**

Date: **November 27th, 2023**

From (source): TC CYBER
CYBER(23)35d008r1

Contact(s): Alex Leadbeater (Maketh Secure), Chair; alex@makethsecure.com
Roger Eriksson (Advenica AB), Rapporteur: roger.eriksson@advenica.com
Laure Pourcin (ETSI), Technical Officer; laure.pourcin@etsi.org; cybersupport@etsi.org

To: GSMA FASG, GSMA 5GMRR, GSMA 5GPKIWP

Copy to: 3GPP SA2, 3GPP SA3

Response to: (if applicable) **CYBER(36)**

Attachments: (if applicable) ETSI TS 103 523-2 V1.1.1

1. Overall description

TC CYBER has observed the Liaison Statement S3-234467 from GSMA to 3GPP TSG SA3 and the corresponding reply S3-235009. A number of groups within ETSI, have invested large efforts into studies and normative work on the topic of inspection of encrypted traffic and would like to provide some comments for GSMA consideration.

2. Background

The migration from TLS1.2 to TLS1.3, while providing many desirable security enhancements, has negatively impacted existing solutions for network-based monitoring (including e.g. IDS, malware protection, data leakage prevention, fault detection, audit, etc) in terms of added complexity and/or a need to resort to methods that break the end-to-end principle more than one would like, e.g. also breaking end-to-end authenticity. ETSI has therefore developed a suite of protocols (the TS 103 523 series) addressing various aspects of this problem space.

According to the aforementioned GSMA-3GPP Liaison Statements, GSMA has considered ETS, 103 523-3, but discarded it due to the potential security downgrade arising from a front-end proxy to the remote server. TC CYBER has no reason to question this analysis. GSMA instead proposes the so called "Option 2" in which the signaling payload session maintains its end-to-end security properties, and a mirror copy of this session is sent (secured) to the Monitoring System(s). TC CYBER has taken the liberty of borrowing the Figure below from S3-234467.

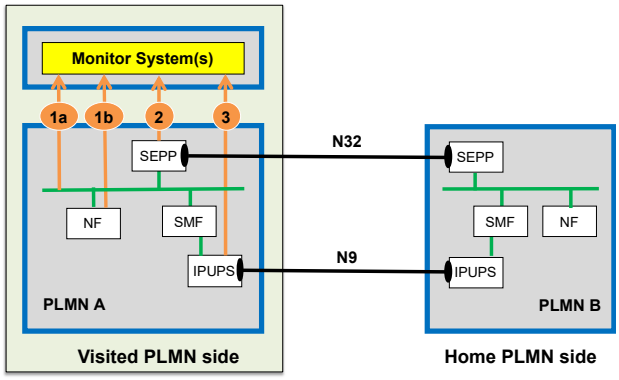

Figure (reproduced from S3-234467).

TC CYBER would like to draw GSMA's attention to what could be a significant problem with Option 2 and would also like to point to another protocol within the TS 103 523 series which might address GSMA's concerns about ETS, while at the same time avoiding the issues with Option 2.

3. Potential problem with Option 2

The understanding of TC CYBER is that the need for monitoring of signaling traffic is to support surveillance, error diagnostics, etc. For such tasks to be of relevance, it needs to be assumed that the network entities generating the traffic (SEPP, PLMN-internal NF, etc), might have implementation errors or might be subject to other random or even intentional error conditions (e.g. malware or adversarial take-over). Under none of these conditions can it be assumed that the traffic mirror copy sent to the Monitoring System is identical to the traffic forwarded to the other PLMN. Surely, in the case of a hostile infiltration into the PLMN, the attacker would ensure that the traffic sent to the Monitoring System appears legitimate. In the view of TC CYBER, this appears to raise doubts on the effectiveness of Option 2.

4. Other alternatives: TLMSP

TC CYBER would like to bring to the attention of GSMA, another protocol within the 103 523 series, namely the Transport Layer Middlebox Security Protocol (TLMSP), TS 103 523-2 [1]. This protocol avoids the potential issues with Option 2 as discussed above since it places the Monitoring System "on-path" with the actual signaling traffic. TC CYBER also believes it could address many of the concerns that GSMA raised with ETS. For example:

- With TLMSP, the proxy (Monitoring System) cannot step into the secured session without having been explicitly authenticated/authorized by the endpoint(s).
- End-to-end authentication can be maintained.
- Authorization to signaling content can be fine grained, e.g. only allowing access to certain parts (similar to the 3GPP PRINS protocol).
- Authorization can be granted for specific purposes only. E.g. "read" access can be granted while preventing "write/modify" access by the intermediate systems (again, akin to PRINS).

TLMSP should be well suited, especially for the N32 connection in the figure above.

5. Actions:

TC CYBER provides the above information for consideration by GSMA and is happy to liaise further, if so desired.

6. References

[1] TS 103 523-2, "CYBER; Middlebox Security Protocol; Part 2: Transport layer MSP, profile for fine grained access control",
www.etsi.org/deliver/etsi_ts/103500_103599/10352302/01.01.01_60/ts_10352302v010101p.pdf

7. Date of next meetings of the originator

- CYBER#36 December 6 – 8, 2023, Sophia Antipolis, France
- CYBER#37 February 21 – 23, 2024, Sophia Antipolis, France