**3GPP TSG-SA3 Meeting #115 *draft\_S3-240892-r1***

Athens, Greece, 26th February - 1st March 2024

**Title: Reply LS on CVD-2023-0079 – Lack of GPRS IOV randomisation**

**Response to: LS on CVD-2023-0079 – Lack of GPRS IOV randomisation from GSMA CVD PoE**

**Source: 3GPP TSG SA WG3**

**To: GSMA CVD PoE**

**Cc: 3GPP TSG CT WG1**

**Contact person: Vlasios Tsiatsis**

**vlasios dot tsiatsis at ericsson dot com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:** S3-24XXXX

# 1 Overall description

SA3 would like thank the GSMA CVD PoE for the LS CVD-2023-0079 – Lack of GPRS IOV randomisation.

The LS mentions an unnamed commercial GPRS network, which was found to be using a default IOV value at the start of each GPRS session and thereby reducing the strength of GPRS encryption. The GSMA CVD PoE includes recommendations for specifications under the responsibility of 3GPP CT1 and 3GPP SA3.

3GPP SA3 has discussed the recommendations provided by the GSMA CVD PoE and has agreed on the attached CRs.

3GPP SA3 would like to request the GSMA CVD PoE to take the information into account.

# 2 Actions

**To GSMA CVD PoE**

**ACTION: 3GPP SA3 would like to request the GSMA CVD PoE to take the information into account.**

# 3 Dates of next TSG SA WG 3 meetings

SA3#115AdHoc-e 15 - 19 April 2024 Electronic meeting

SA3#116 20 - 24 May 2024 Jeju (South Korea)

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)