GSMA Security Accreditation Scheme

Accredited Supplier

Certificate No: AR-IN-UP-0723

# Certificate

This is to certify that

Amkor Technology Korea, Inc. - K3, Incheon, Korea

has participated in the GSM Association Security Accreditation Scheme for UICC Production (SAS-UP) and satisfied the scheme's requirements.

This certificate remains valid until the end of July 2023*.

Alex Sinclair
Chief Technology Officer
GSMA

* Dependent on continued supporting site certification (currently valid to end June 2023 & July 2023)

Check certificate validity: A list of accredited sites is published on the GSM Association website at www.gsma.com/sas/

Security Accreditation Scheme

Accredited Supplier

# Scope of Certification

To be viewed as part of Security Accreditation Scheme Certificate No: AR-IN-UP-0723

## Production Site: Amkor Technology Korea, Inc - K3

**Site Address:** Bupyeong, 110 Anaji-ro, Gyeyang-gu, Incheon 21107, Republic of Korea

**Supporting site(s) details:**

**Type: Logistics operations, reject materials storage. Amkor Technology Korea – K3 logistics centre, 64 Annam-ro 418 Beon-gil, Bupyeong-gu, Incheon, Republic of Korea. Expiry date: July 2023**

**Type: Generation of hardware security credentials, control of Perso_SC process. Qualcomm Technologies, Inc., 5775 Morehouse Drive, San Diego, CA 92121, USA. Expiry date: June 2023**

The auditors were provided with appropriate evidence that the processes and controls on the audit dates were consistent with those required by the SAS-UP Standard v*9.1* and the SAS Consolidated Security Requirements v*8.1*, with the following scope:

| | | | |
|---|---|---|---|
| **Generation of data for personalisation:** | Not carried out at this site | **Personalisation:** | 2-step personalisation: Perso_SC |
| **Management of PKI certificates:** | Not carried out at this site | **Post-personalisation packaging:** | Not carried out at this site |

**Notes & Exclusions:** Perso_SC production data is delivered to Amkor's K3 site by a single customer directly to a customer-supplied and managed IT environment. Data is used during production by an Amkor tester running a customer-supplied test program. Sensitive data is encrypted end-to-end from generation at the customer site to the point of writing into the target device by its loader function. The encryption and decryption mechanisms and all key handling are controlled by the customer organisation and treated as a black-box by Amkor K3. Amkor K3 does not directly handle keys used to protect production data and has no access to decrypt production data. Key handling was not in scope of this site's audit.

Due to the Covid-19 pandemic travel restrictions the audit was performed remotely in accordance with the GSMA SAS Covid-19 Audit and Certification Policy. An assessment of compliance with requirements that could not be audited fully remotely will need to be performed as part of a follow-up physical audit after Covid-19 related disruption to on-site SAS audits has ended.

**For and on behalf of FML**
(James Messham)

**For and on behalf of ChaseWaterford**
(Vernon Quinn)

SAS certification is awarded based on an assessment by the audit team that the site met the requirements of the SAS Standard during the audit, and that it demonstrated an ability and intent to sustain compliance during the certification period. Continued site compliance with the SAS Standard during the certification period, including the implementation of SAS-compliant controls following any changes to the certified environment, is the responsibility of the site. This certificate cannot guarantee that the above organisation is invulnerable to attack or breaches of security. GSMA, FML and ChaseWaterford exclude all liability for loss or damage of any description caused by any failure or breach of the above organisation's security save as may be required by law.