GSMA Security Accreditation Scheme

Accredited Supplier

Certificate No: SE-TG-UP-1223

Provisional Certificate

This is to certify that

Siliconware Precision Industries Co. Ltd., Taichung, Taiwan

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

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

Alex Sinclair
Chief Technology Officer
GSMA

* Dependent on continued supporting site certification (currently valid to end June 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 Provisional Certification

To be viewed as part of Security Accreditation Scheme Certificate No: SE-TG-UP-1223

Production Site: **Siliconware Precision Industries Co. Ltd., Zhong Ke Facility**

Site Address: **No. 19, Keya Rd., Daya, Taichung, Taiwan 428, ROC**

Supporting site(s) details: **Type: Generation of Perso_SC data & control of Perso_SC process via systems installed at the SPILZK site. Qualcomm San Diego, 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*9.0*, with the following scope:

Generation of data for personalisation:	Not carried out at this site	**Personalisation:**	Embedded; 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: Production data for Perso_SC is delivered to SPILZK site by a single customer directly to a customer-supplied and managed IT environment hosted at SPILZK. Data is used during the production process by a SPILZK tester running a customer-supplied test program. Sensitive data is encrypted end-to-end from the point of generation at the customer site to the point that it is written 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 SPILZK. SPILZK does not directly handle keys used to protect production data and has no access to decrypt production data.
Key handling has not been considered within the scope of this site's audit.

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.