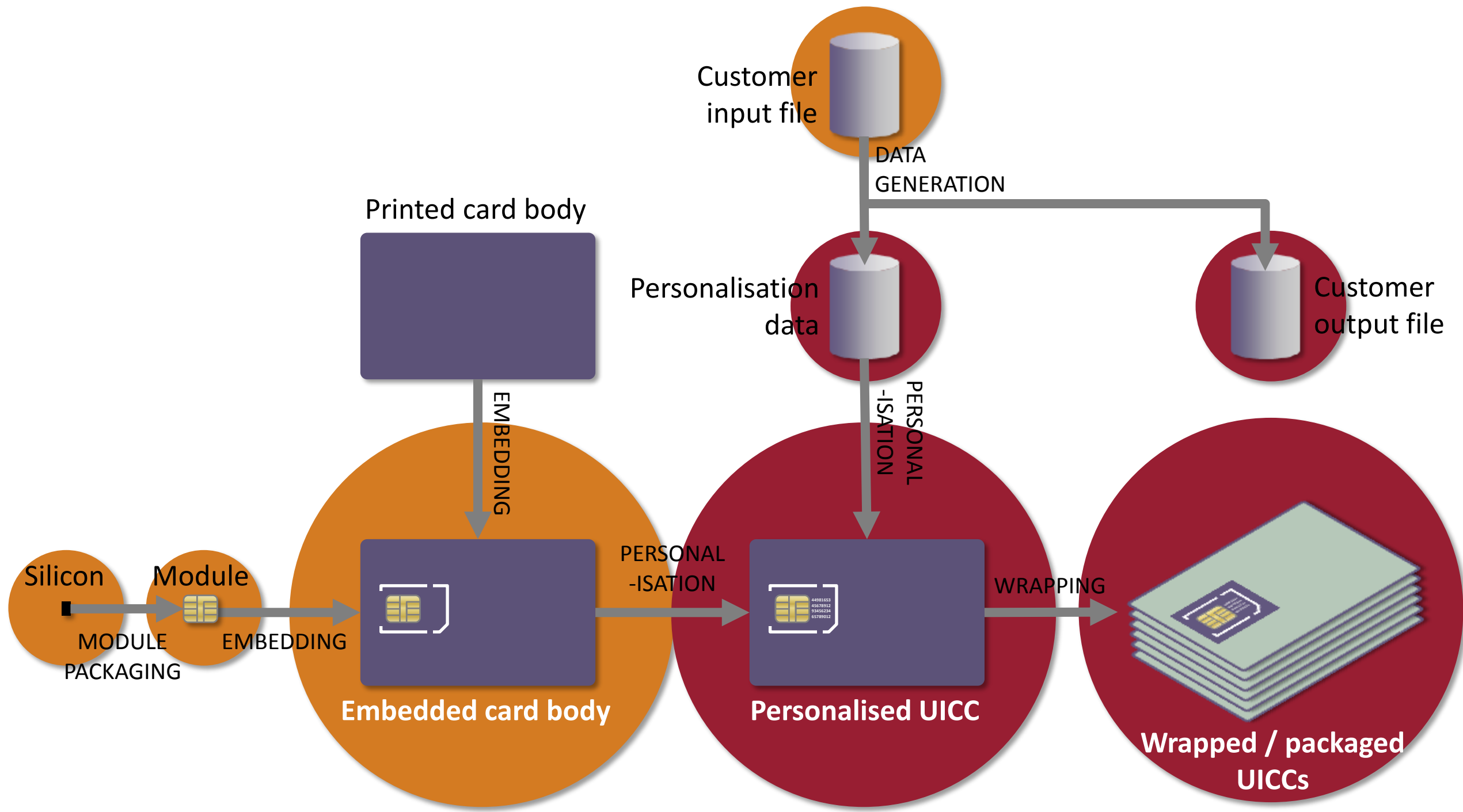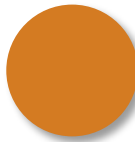# Guide to using SAS for GSM Operators

To help GSM operators interpret certificates issued by the GSM Association as part of the Security Accreditation Scheme (SAS) for smartcard suppliers, the following points should be considered:

	Certified site	Scope of certification	Certificate status and expiry
Background	An SAS certificate is issued to apply to one specific manufacturing site. The site is specified on the certificate itself. In some cases manufacturers may conduct UICC manufacturing at more than one site. Separate certificates will be issued for each site certified as meeting the requirements of SAS. Sites for which no certificate has been issued are not certified as compliant with the requirements of SAS. Some manufacturers are known to outsource some of their UICC manufacturing to other sites or third parties. Outsourced production is not within the SAS certificate scope.	The UICC manufacturing process comprises a number of stages (see diagram overleaf). Not all SAS certified sites conduct all processing stages. All processing stages conducted at an SAS certified site will be within the scope of an SAS audit. Any processing that is subcontracted to third part suppliers will not be within scope. Different parts of the process involve different risks. SAS considers those processes involving Class 1 assets to be the highest risk and require the greatest controls. Processes involving lower sensitivity Class 2 assets represent a slightly lower risk, and unclassified assets a much lower risk.	Each SAS certificate is issued for a defined period. The first certificate for a new site will normally be issued for 1 year. Renewal certificates for existing sites will normally be issued for 2 years, however in some circumstances may be shorter. SAS provides certified sites with a mechanism to ensure that certification is continuous, however this is dependent on each site requesting and scheduling its audits in time.
Recommended actions	Operators issuing tender documents for UICC manufacturing should seek to confirm that the price quoted in any tender response applies specifically to production at a certified manufacturing site. Operators should satisfy themselves that their UICCs will be manufactured at an SAS certified site, obliging this contractually where considered appropriate.	All operators seeking SAS compliance from their suppliers should aim for data generation and personalisation to be within the certificate scope. Again, ensuring that production at a certified site is part of the contract is critical. Operators requiring value-added packaging should consider the need for SAS compliance carefully. Packaging is often outsourced, either by the UICC supplier, or by the operator itself. Third parties carrying out value-added packaging are often strongly cost driven, with poor security controls. In contrast SAS requires full auditability of, and accountability for, sensitive materials in the packaging process. Operators requiring the highest level of security for their manufacturing should target all Class 1 processes to be carried out at SAS certified sites.	Operators should track the certification expiry dates of their suppliers, and subscribe to the GSM Association's email notification for changes to site certification. Again, obliging suppliers to maintain certification contractually is advisable.

Customer input file

DATA GENERATION

Printed card body

Personalisation data

Customer output file

EMBEDDING

PERSONAL-ISATION

Silicon

Module

PERSONAL-ISATION

WRAPPING

MODULE PACKAGING

EMBEDDING

Embedded card body

Personalised UICC

Wrapped / packaged UICCs

Unclassified SAS assets (low value/risk)

SAS Class 2 assets (intermediate value/risk)

SAS Class 1 assets (highest value/risk)