December 2021

Qualcomm

GSMA SAS Addressing *Perso_SC* scalability

Or Elnekaveh

Software/Security Architect – SPU team

Problem description

The number of audited SAS-UP required by Integrated eUICC Perso_SC scope

- (Removable) UICC — *high* volume – *few* manufacturers
- Discrete eUICC — (following a similar path)
- Integrated eUICC Perso_**UICC** — Limited number of sites

→ **Few SAS-UP audited sites**

- Integrated eUICC Perso_**SC**: **large number of sites (difficult to scale)***
  - Multiple business segments (mobile, compute, automotive, wearable, IoT)
  - Multiple tiers (e.g., premium, high, mid, low)
  - Fast pace of change (e.g., an annual cadence, derivative chips)
  - Fabless SoC makers, multiple manufacturing sites: fabs and (Outsourced) **S**emiconductor **A**ssembly and **T**est (SATs): different entities, different countries.

→ ***{segments} X***
{tiers} X
{cadence} X
{SATs}

* Complex logistics and indirect costs

Self-generation: Reducing the number of SAS-UP audited sites

Addressing scalability of Integrated eUICC Perso_SC *Two-step Personalisation*

Recap: **Two-Step** Personalisation

A process defined by FS.17/18 for Integrated eUICC

SAS Accredited sites

Entry / Symbol	Certification Type	Scope
UICC | UICC^P		Within scope (UICCs)
eUICC | eUICC^P		Within scope (eUICCs)
① 2:SC | 2:SC^P		Within scope (2-step personalisation – Perso_SC)
② 2:UICC | 2:UICC^P	Full | Provisional	Within scope (2-step personalisation – Perso_UIC
C | C^P		Within scope (card form factor)
E | E^P		Within scope (embedded form factor)
W | W^P		Within scope (Wafer Level Chip Scale Packaging
✓	N/A	GSMA PKI Live; site has demonstrated compliant certificate(s) in use*.
✓	N/A	GSMA PKI Ready; site has demonstrated compliance certificate management with non-GSMA PKI certi
-	N/A	Not carried out at this site

GSM Association
FS.18 - Security Accreditation Scheme - (

Non-confidential

GSMA FS.17/18 Section 11

Statements from CSR			Guidelines	
11 Two-step personalisation process				
I		Personalisation may be carried out as a two-step process (Perso_SC and Perso_UICC). The process may involve a different entity in each step. SAS-UP requirements apply to both personalisation steps. SAS-UP certification must be applied to each step for UICC production flows requiring SAS-UP compliance (e.g. eUICC). SAS-UP assessment of two-step personalisation process can currently only be applied to the following produc • In		Requirements for the two-step personalisation process are not intended to apply where the full personalisation process takes place in the same physically-secure EUM environment. Requirements in this section have been added to enable SAS-UP to support products, such as Integrated UICC, where the two personalisation steps may be carried out at different times, potentially in different environments under the control of different entities. Production processes for product types other than those listed in this requirement are not currently supported for SAS-UP certification, although this may change in the future. …ain will be expected to demonstrate
	11.1			
	11.1.1	…controls to ensure that: • Personalisation data is only used once. • Creation of duplicate devices containing the same personalisa		…preventing duplicate production; each set of credentials generated should exist and be used in exactly one instance.
	11.2	Generation of hardwa		
	11.2.1	The generation of har… and their provisioning… shall be considered a… evaluated according t… section 7 of this docum…		…and …are FIPS …occur in separate facilities, a secure exchange mechanism should be in place.

Implementation is intentionally undefined.

Auditees must demonstrate to the auditors that their solutions are compliant with the requirements.

V7.0

Page 81 of 84

Recap: **Two-Step** Personalisation

Each step can be performed by a different entity

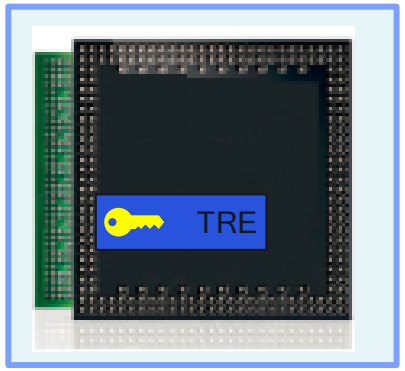
Step #1: Perso_SC scope

- Generation and provisioning of *hardware security credentials*
- e.g. TRE attestation keys/certificate

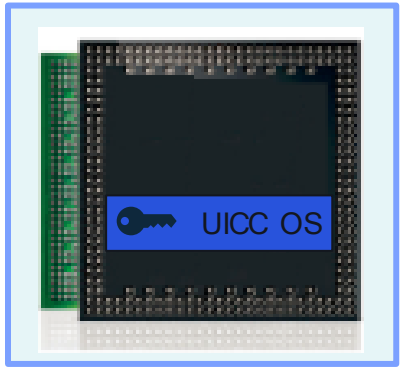
Step #2: Perso_UICC scope

- Generation and provisioning of *UICC OS credentials*
- Supports injection or on-device generation
- e.g. RSP EUICC and EID

① TRE Manufacturer



② UICC OS Maker

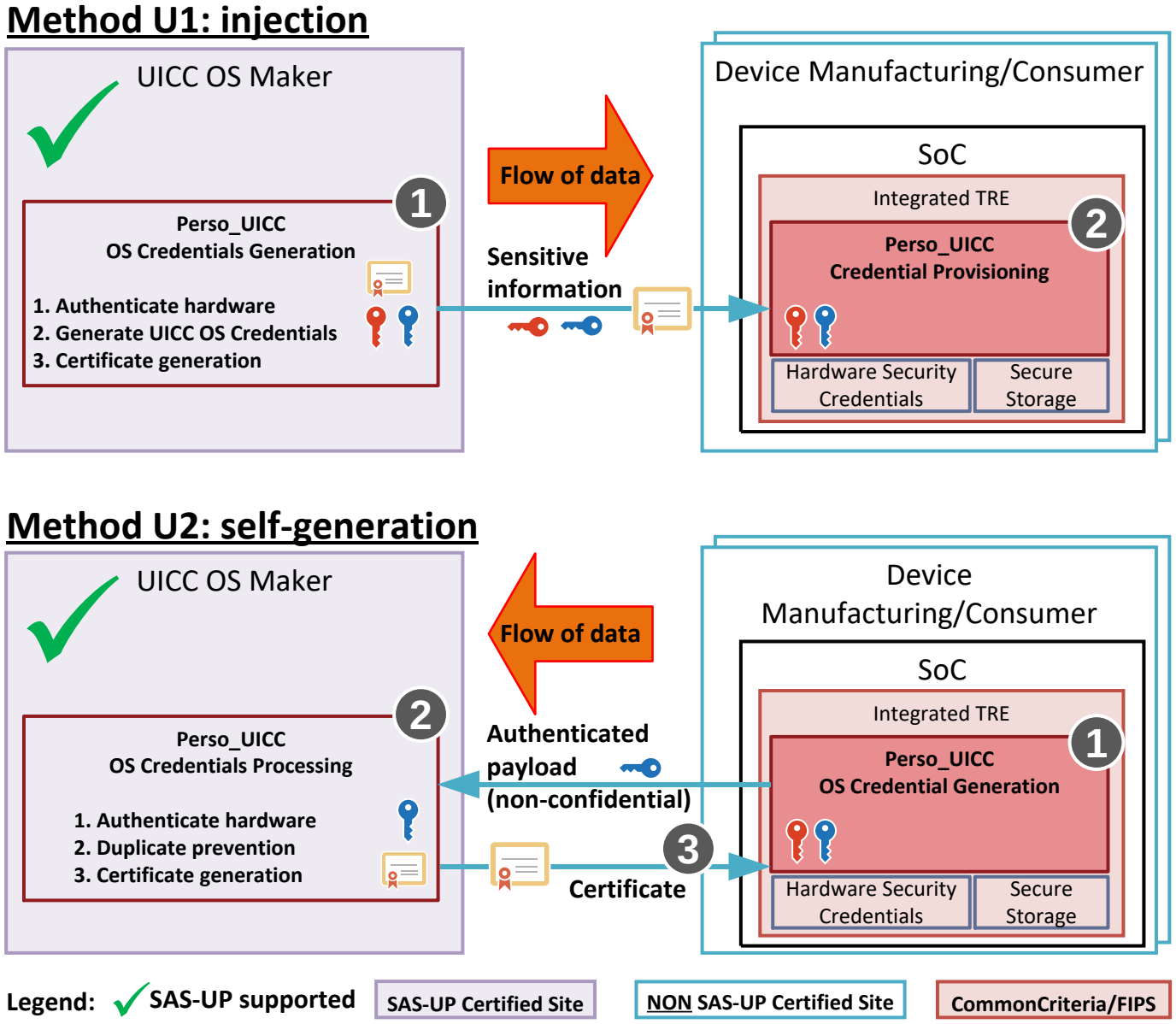


Step #2: Perso_UICC

Supported methods

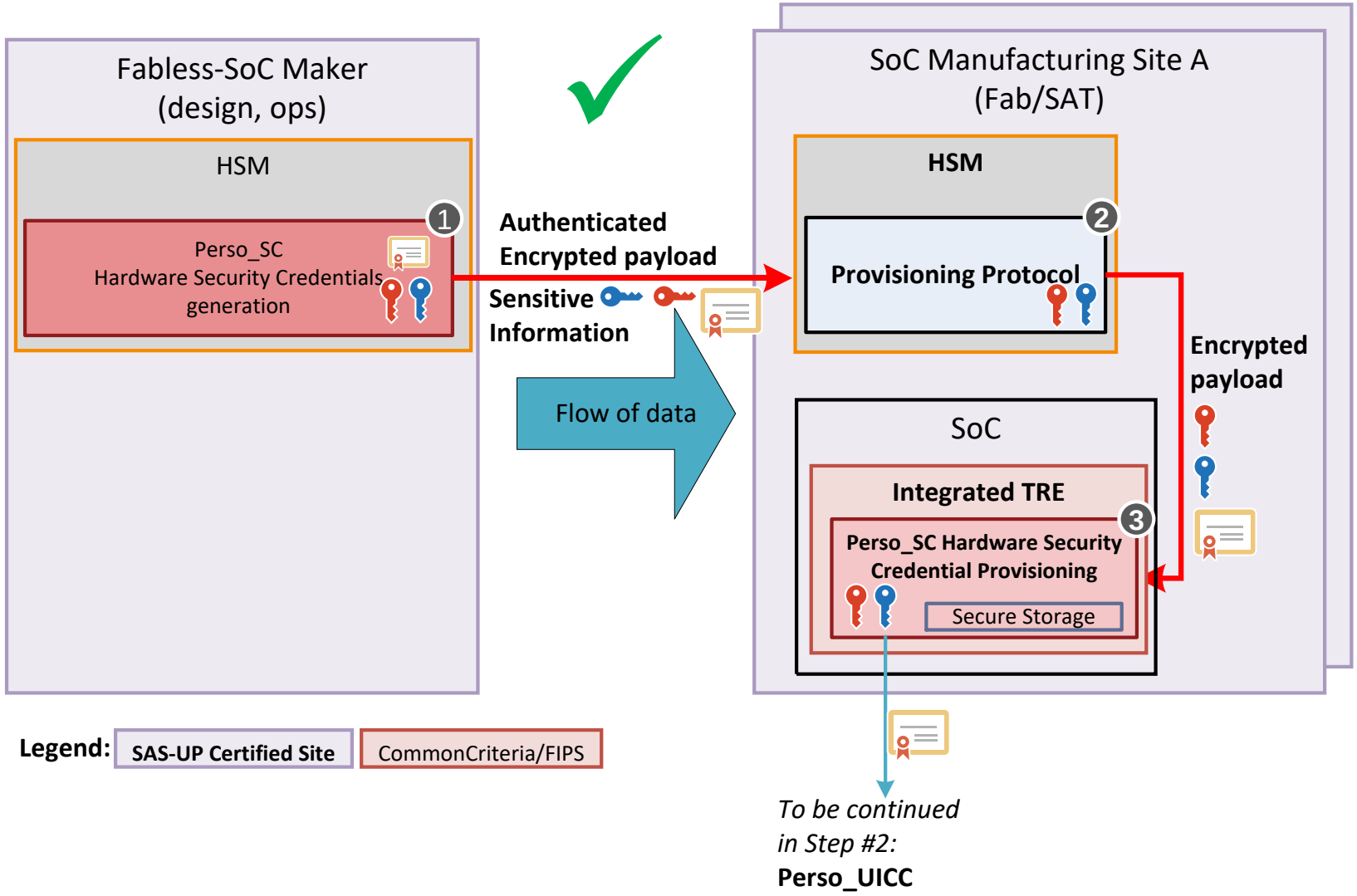
- U1: generate OS credentials outside TRE and *inject* in a non-SAS-UP certified site

- U2: **self-generate** sensitive OS credentials **within** TRE, and *obtain* a certificate in a non-SAS-UP certified site



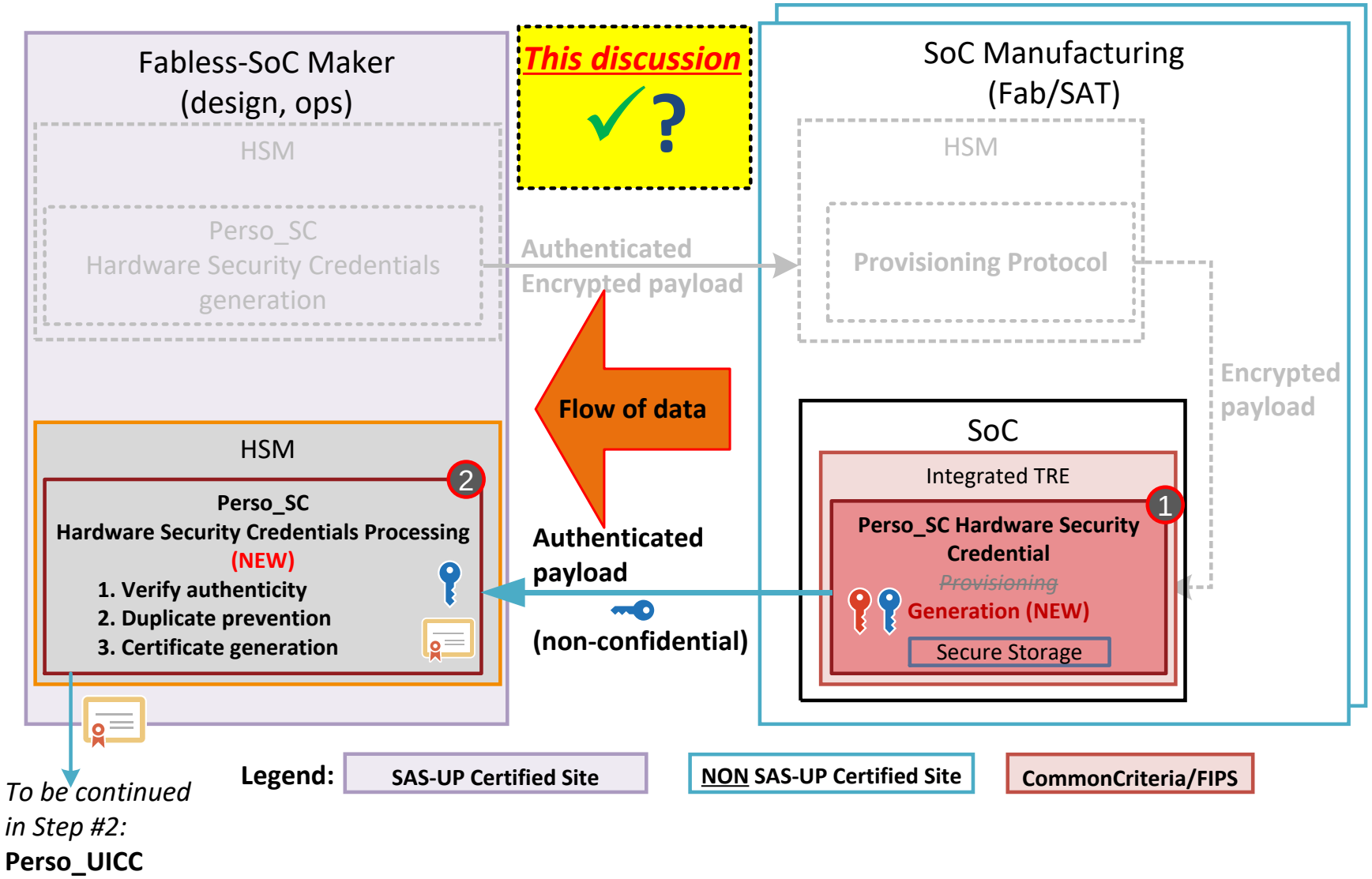
Step #1: Perso_SC method S1 (injection)

- **Injection of sensitive information**
- **Both** sites are SAS-UP certified.
- SAS: covers generation and provisioning
- eUICC: Once provisioned: Confidentiality covered by CommonCriteria



Step #1: Perso_SC method S2 (self-generation)

- **Sensitive Perso_SC credentials do not leave Integrated TRE**
- Data transfer: Authentication required. Confidentiality not required.
- **Manufacturing sites - not SAS-UP certified**



Comparison between Perso_SC methods

(generating Integrated TRE Hardware Security Credentials)

	Method S1 (injection)	Method S2 (self-generation)
Credentials generation	FIPS 140-2 compliant	
Generation location	Outside TRE	Inside TRE
Transfer of sensitive information	Yes	No
Authentication	Yes	
Direct impact on Perso_UICC (Step #2)	No	
Protection of provisioned credentials	According to product security, e.g., as defined by eSIM (SGP.21 Annex J)	

Conclusion: auditees could use S1 or S2 to demonstrate the same level of trust

No change in FS.17/18

Already covered by current high-level language

GSMA FS.18

Statements from CSR			Guidelines	
11 Two-step personalisation process				
I		Personalisation may be carried out as a two-step process (Perso_SC and Perso_UICC). The process may involve a different entity in each step. SAS-UP requirements apply to both personalisation steps. SAS-UP certification must be applied to each step for UICC production flows requiring SAS-UP compliance (e.g. eUICC). SAS-UP assessment of two-step personalisation process can currently only be applied to the following product types: • Integrated eUICC		Requirements for the two-step personalisation process are not intended to apply where the full personalisation process takes place in the same physically-secure EUM environment. Requirements in this section have been added to enable SAS-UP to support products, such as Integrated UICC, where the two personalisation steps may be carried out at different times, potentially in different environments under the control of different entities. Production processes for product types other than those listed in this requirement are not currently supported for SAS-UP certification, although this may change in the future. Auditees involved in the eUICC production chain will be expected to demonstrate that the combined solution is secure.
	11.1	Control of duplicate production		
	11.1.1	Each personalisation step shall incorporate controls to ensure that: • Personalisation data is only used once. • Creation of duplicate devices containing the same personalisation data is prevented.		Auditees should demonstrate controls for preventing duplicate production; each set of credentials generated should exist and be used in exactly one instance.

GSMA FS.18

Statements from CSR			Guidelines	
	11.2	Generation of hardware security credentials		
	11.2.1	The generation of hardware security credentials, and their provisioning into the device hardware shall be considered a sensitive process, and be evaluated according to the requirements in section 7 of this document.		Auditees must demonstrate that hardware credentials are generated and provisioned in a secure manner. Credentials should be generated using security modules (HSM) that are FIPS 140-2 level 3 certified. Where generation and provisioning to Integrated eUICC hardware occur in separate facilities, a secure exchange mechanism should be in place.
	11.3	Personalisation of security credentials (Perso_SC)		
	11.3.1	The personalisation of a hardware device with security credentials shall be considered a sensitive process, and be evaluated according to the requirements in section 7 of this document.		Auditees should demonstrate that hardware credentials are provisioned in a secure manner.
	11.3.2	Perso_SC can occur only once within the device lifecycle.		Auditees should demonstrate that hardware credentials can be provisioned only once.
(Perso_UICC follows)				

Next action

No FS.17/18 change: Integrated eUICC **SAS-UP auditees with Perso_SC scope can choose between method S1 (injection) and S2 (self-generation)**

Qualcomm

Thank you

Follow us on:

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog

All data and information contained in or disclosed by this document is confidential and proprietary information of Qualcomm Technologies, Inc. and/or its affiliated companies and all rights therein are expressly reserved. By accepting this material the recipient agrees that this material and the information contained therein will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc. Nothing in these materials is an offer to sell any of the components or devices referenced herein.

©2018-2021 Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.