Infineon

Never stop thinking

The Security Module

Tool Access, IMEI Security, SIM Lock

– Presented by Infineon Technologies Denmark A/S

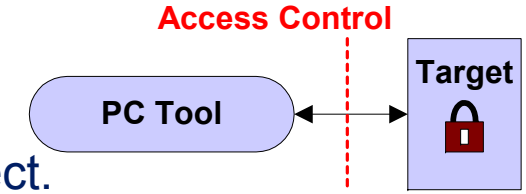
Never stop thinking

Revision: 1.5

Confidential

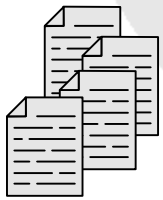
Security Module – Overview

- Tool Access Restriction
  - Only authorized tools are allowed to connect.



- IMEI Security
  - Storing and protection of IMEI to prevent tampering.

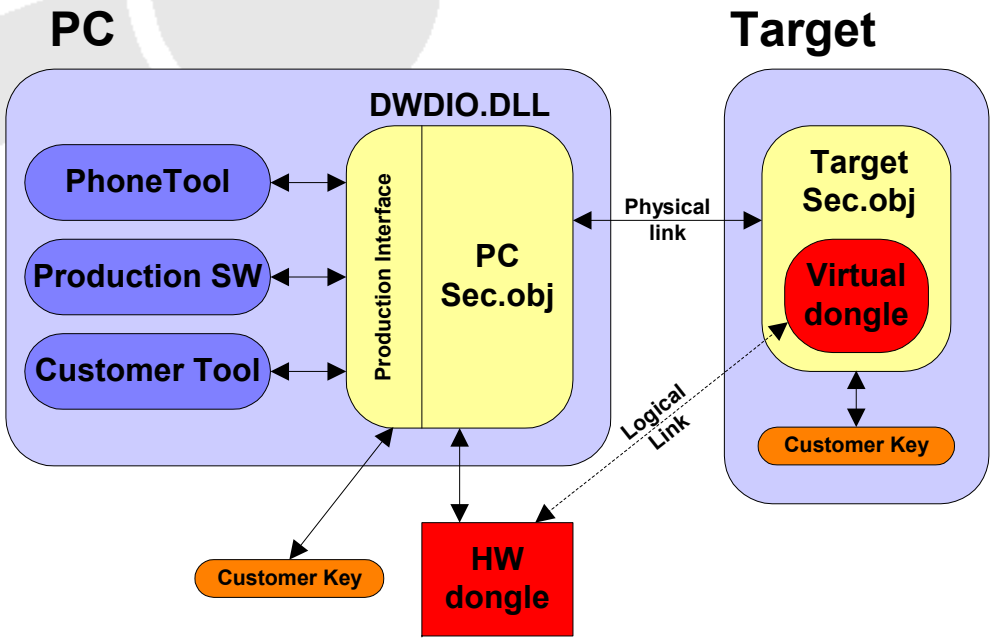
- ME Personalization
  - SIM Locks handling. GSM 02.22.
  - Additional proprietary lock variations and special mechanisms.

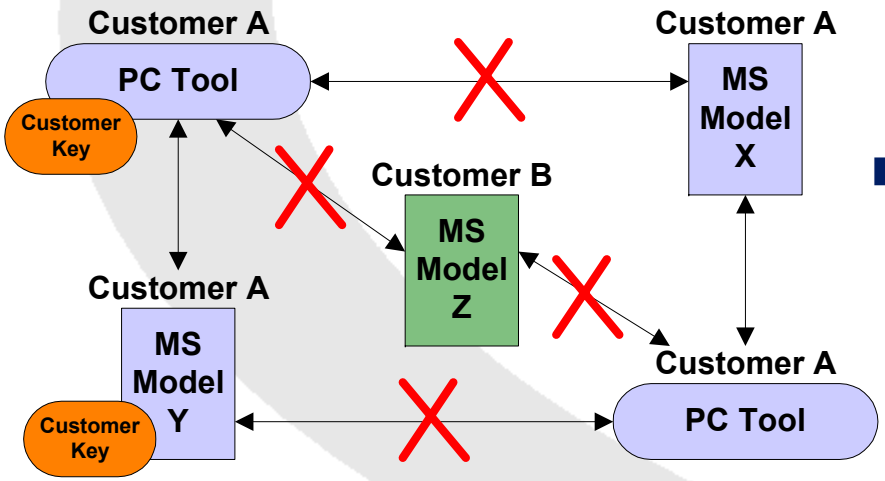


- Overview
  - Personalization Functionality Overview.
  - Customer Delivery Procedure.
  - Security / Standard Solution / Security Library Concept.

Security Module – Tool Access Restriction 1

- Only authorized PC tools can gain access to the ME.
- Special “authentication check sequence” between PC tool and Target.
- Connection check is customer specific:





- A customer key can be applied for further tool access restriction.

Security Module – Tool Access Restriction 2

- The HW dongle, the DWDIO.DLL and the SEC Object (virtual target dongle) are Customer Specific.

  Target access is only granted when a authorized match between these three units has been established.

- A special Globe Version of HW dongle / DWDIO.DLL / SEC Object exists and are used only for internal development and for customer acquisition.

- The HW dongles, the DWDIO.DLL and the SEC Object are delivered by DWD.

Security Module – IMEI Protection

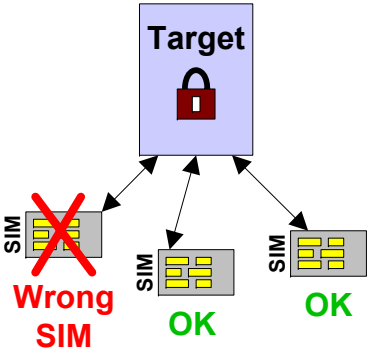
- Store the IMEI (International Mobile Equipment Identity) in a secure and encrypted manner.

- Restrictions on write IMEI
  - Tool Access Restriction (Always).
  - Build Configurations:
    - One time only or multiple time IMEI programming.
    - Optional: Customer specific authentication mechanism for accessing IMEI write functionality.

- Protection of IMEI in flash
  - SEC Default Encryption based on project specific key set.
  - Optional: Customer specific encryption algorithm.

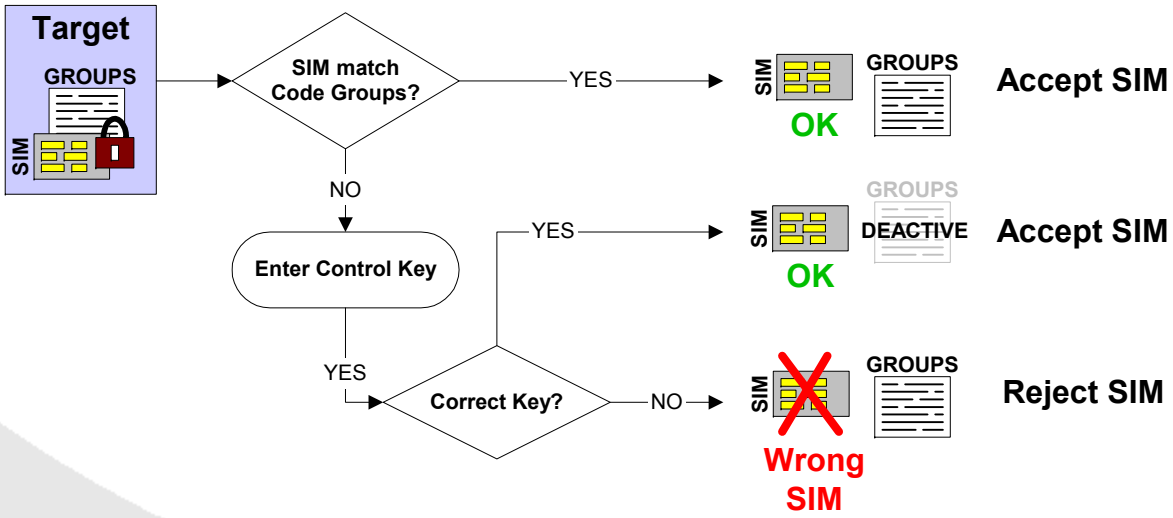
Personalization – The Mechanism

- Personalization is a way of tying the MS to a specific SIM Card or a specific range of SIM cards.



- Codegroups defines the SIM Card acceptance criteria, and are programmed at production.

- The personalized ME validates the SIM card at power-on:

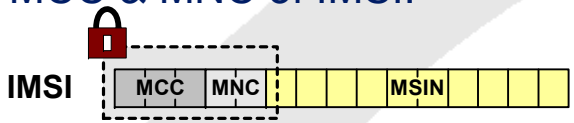


Personalization – The Categories

GSM 02.22 specifies 5 personalization Categories (5 lock types):

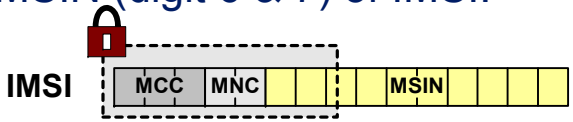
Network Personalization (NO)

~ MCC & MNC of IMSI.



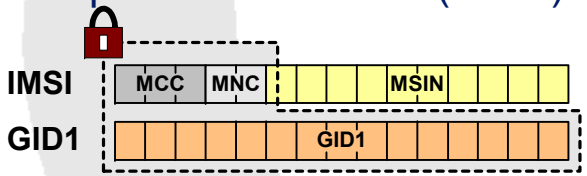
Network Subset Personalization (NS)

~ MSIN (digit 6 & 7) of IMSI.



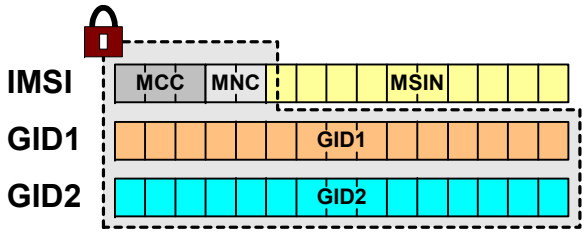
Service Provider Personalization (SP)

~ Group Identifier level 1 (GID1).



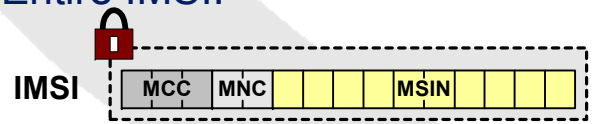
Corporate Personalization (CP)

~ Group Identifier level 2 (GID2).



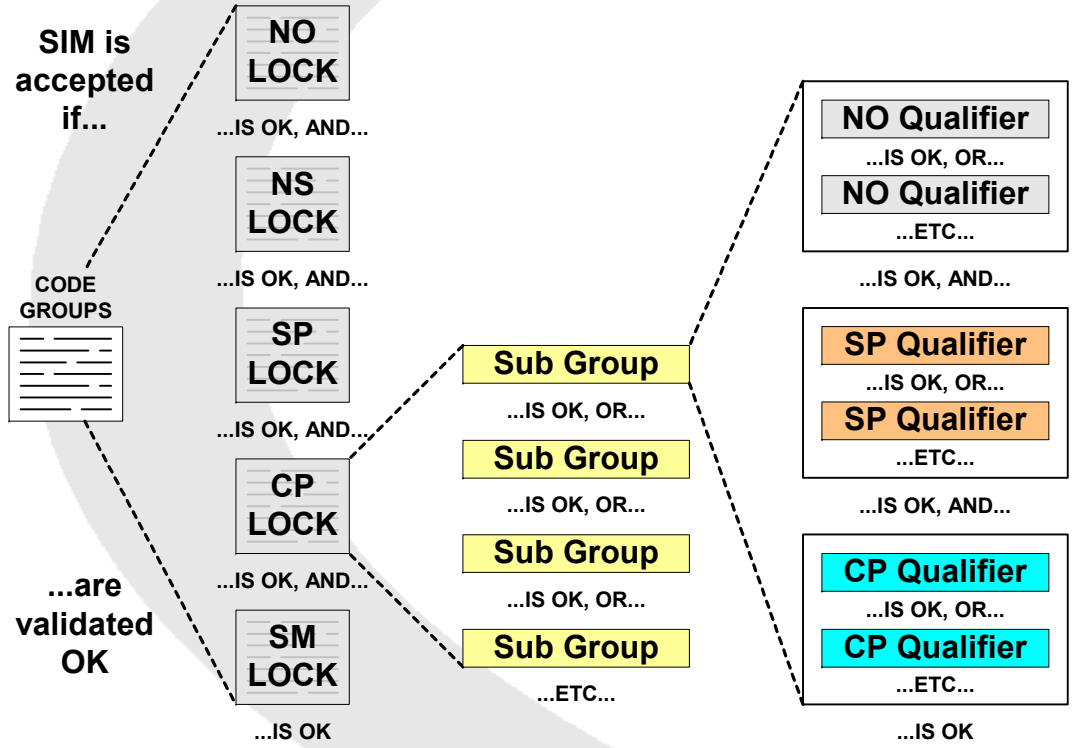
SIM Personalization (SM)

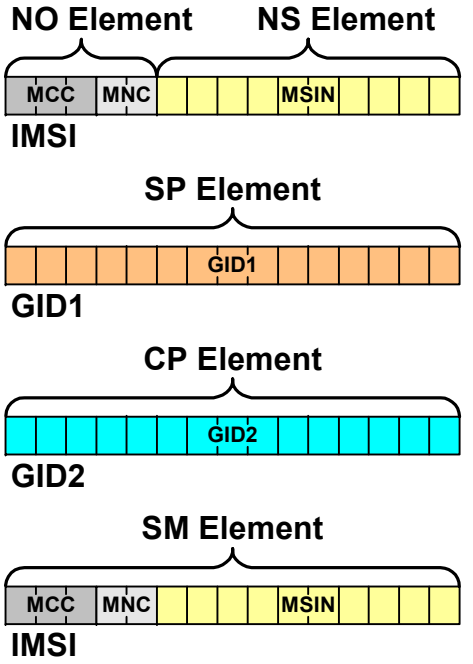
~ Entire IMSI.



Personalization – The Codegroups

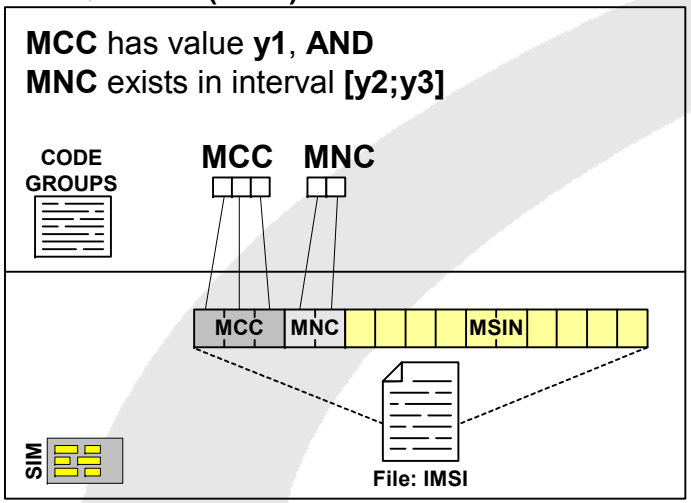
- Categories are split into unique SIM file Elements:
- Qualifiers define a verification rule on one Element.
- The Codegroups are defined and validated this way:



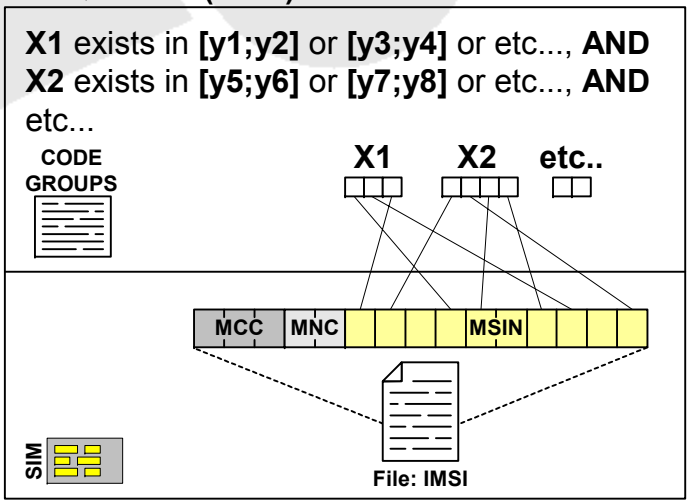


Personalization – The Qualifiers

NO Qualifier (0x02) Definition



NS Qualifier (0x06) Definition



NS Qualifier (0x06) defines up to 9 values X1, X2, etc.

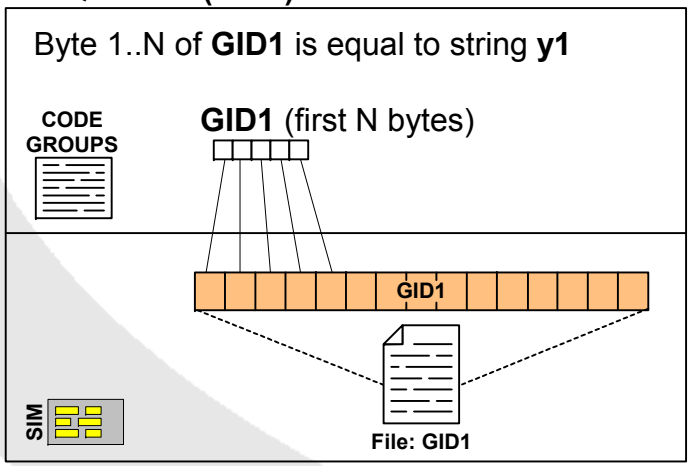
Each value is composed by a set of MSIN digits and must exist in one of up to 15 intervals.

SM Qualifier is similar to SP and CP Qualifier.

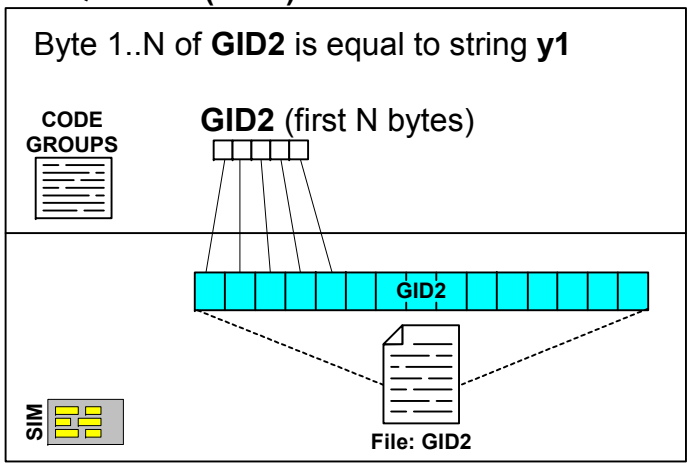
NS Qualifier (0x01) - (0x05) are simplified versions of (0x06).

SP Qualifier (0x02) is similar to (0x01) shown, but allows testing against any other file on the SIM.

SP Qualifier (0x01) Definition

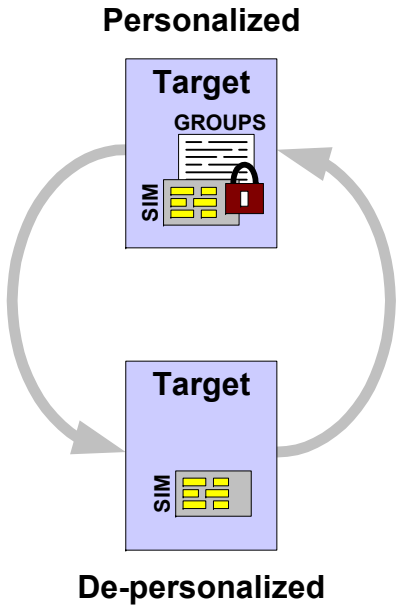


CP Qualifier (0x01) Definition



Personalization – Operation Control

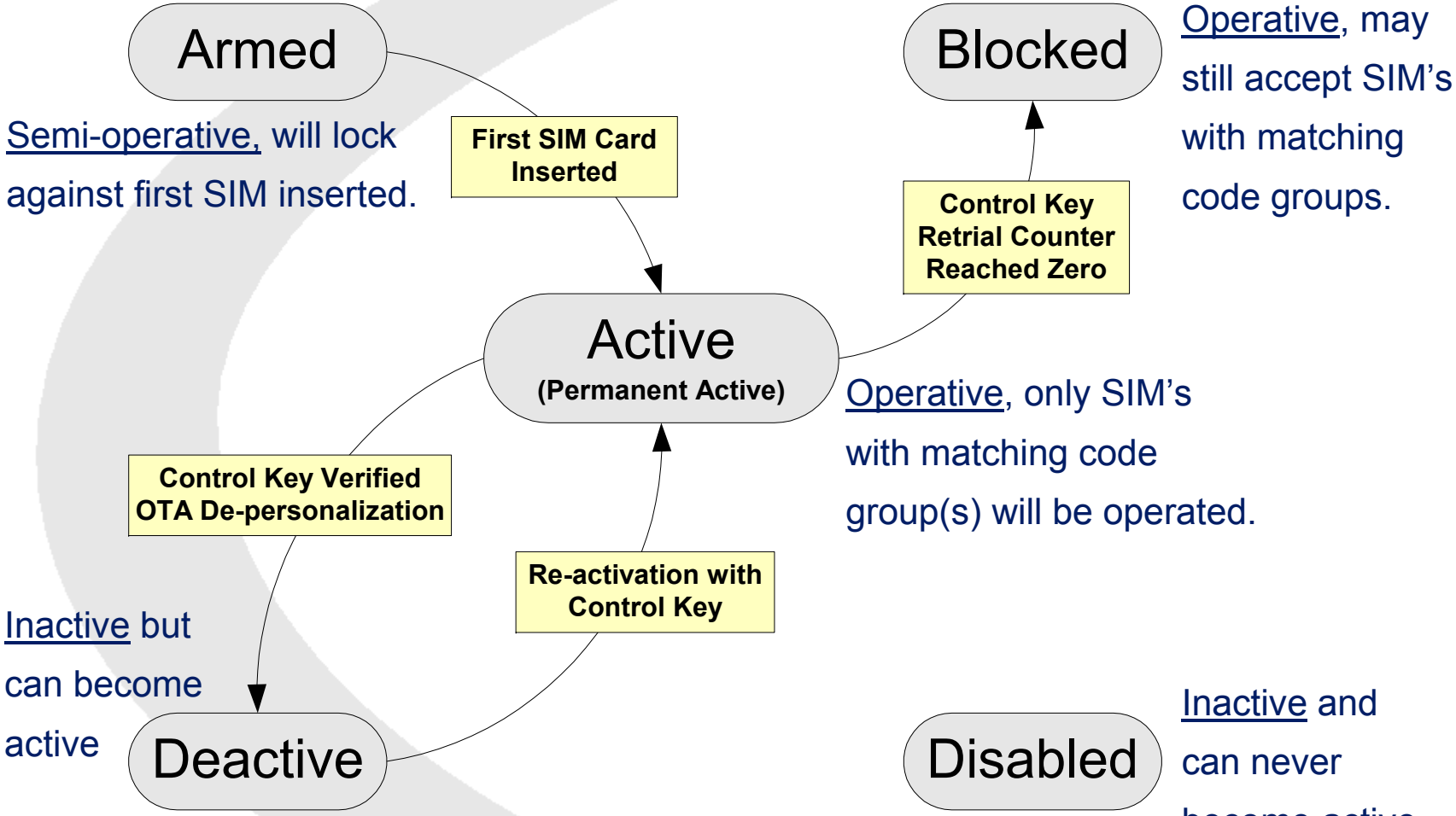
- The ME can become Personalized:
  - During the production phase.
  - At rendezvous with the very first inserted SIM.
  - By the user (using the appropriate control key).



- The ME can be De-personalized:
  - When the appropriate control key (unlock key) has been applied.
  - Using a manufacturer defined de-personalization mechanism.
  - Using the OTA de-personalization procedures:
    - SMS-PP, ME specific.
    - SMS-PP Data Download (utilizing STK Refresh and DCK).

Personalization – Lock States

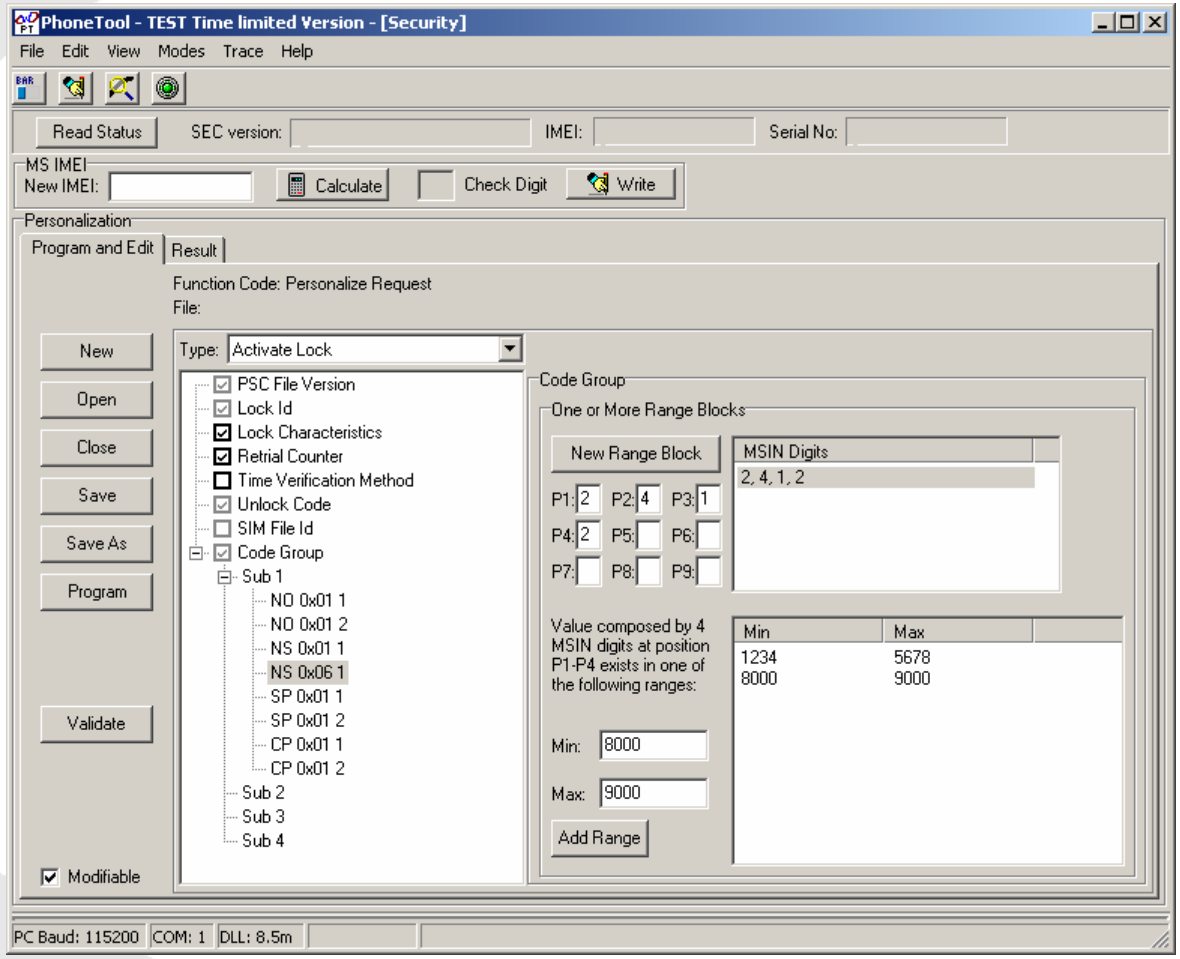
Each of the locks, NO, NS, SP, CP, SM is in one of the states:



Personalization – In Production 1

- PSC Scripts are used for production programming:
  - A PSC script file for every lock NO, NS, SP, CP, SM.
  - A PSC script file for General Settings.
  - Other requests via PSC files.

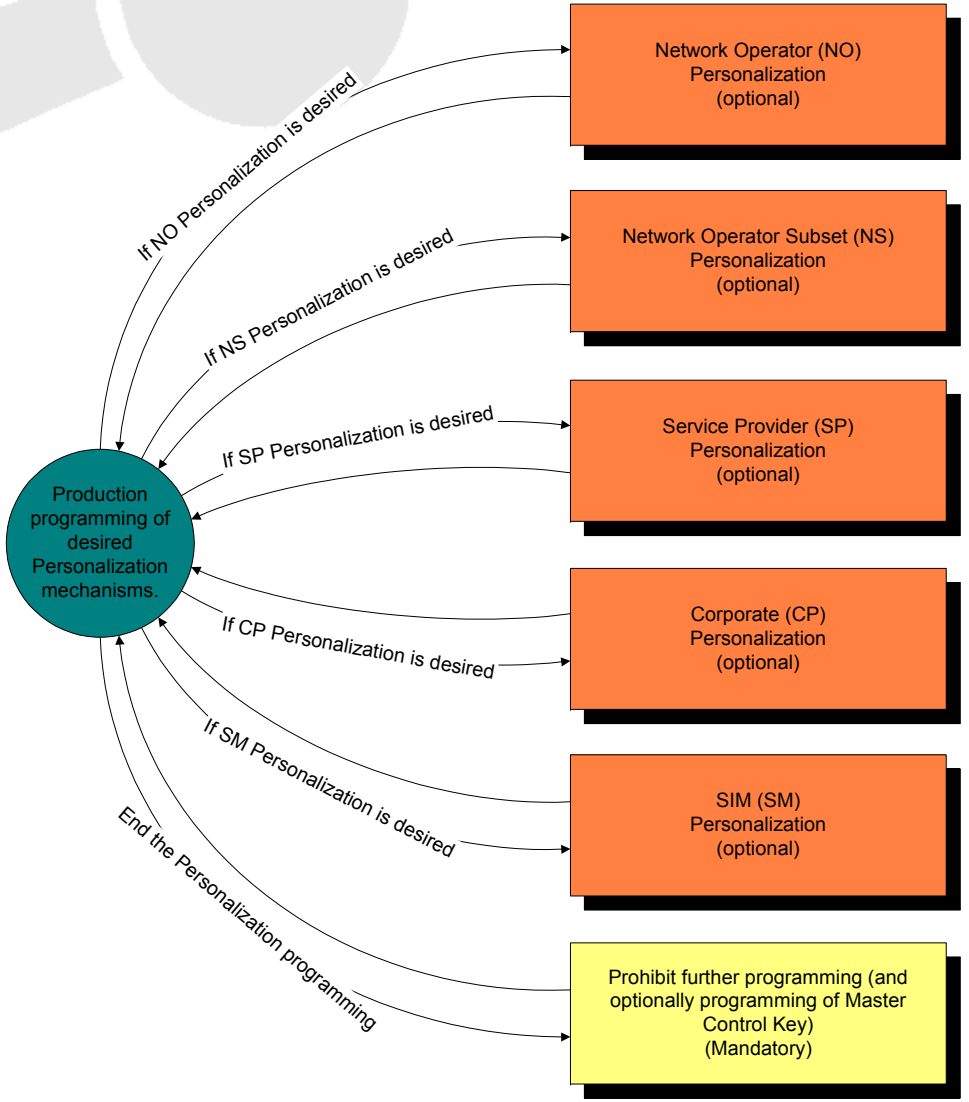
- Phone Tool can be used for generating and programming the PSC Scripts:



Personalization – In Production 2

- Locks are programmed one by one using the PSC script: NO, NS, SP, CP and SM.
- A General Settings PSC script is applied to burn programming 'fuse'.

(A master control key can be set to enable a complete factory re-programming.)



Confidential

Overview – Supported SIM Locks

- GSM 02.22 Locks:
  - NO ~ Network Operator Lock.
  - NS ~ Network Subset Lock.
  - SP ~ Service Provider Lock.
  - CP ~ Corporate Lock.
  - SM ~ SIM (IMSI) Lock.
- Proprietary locks (extension of GSM 02.22 requirements):
  - Vodafone Netherlands.
  - Vodafone D2.
  - Vodafone UK.
  - Vodafone Spain.
  - Vodafone Ireland.
  - SFR.
  - Movistar.

Overview – Personalization

- In factory it is for each of the locks NO,NS,SP,CP,SM possible to:
  - Set lock state to: Armed, Active, Deactive, Disabled.
  - Define a codegroup including subgroups with qualifier rules testing against the SIM file elements.
  - Disable / Enable Unlock Code, Time Limited Verification, Key Retrial Counter, ME Blocking.
  - De-personalization via DCK (OTA de-personalization).
  - Armed Lock: Disable / Enable CNL Arming (arming against elements from CNL list).
- In factory it is possible to set some of the general settings:
  - Disable / Enable Test SIM Acceptance.
  - Disable / Enable One common unlock key for all locks.
  - Disable / Enable Master Control Key (disabled, means factory reprogramming of SIM locks will newer be possible)

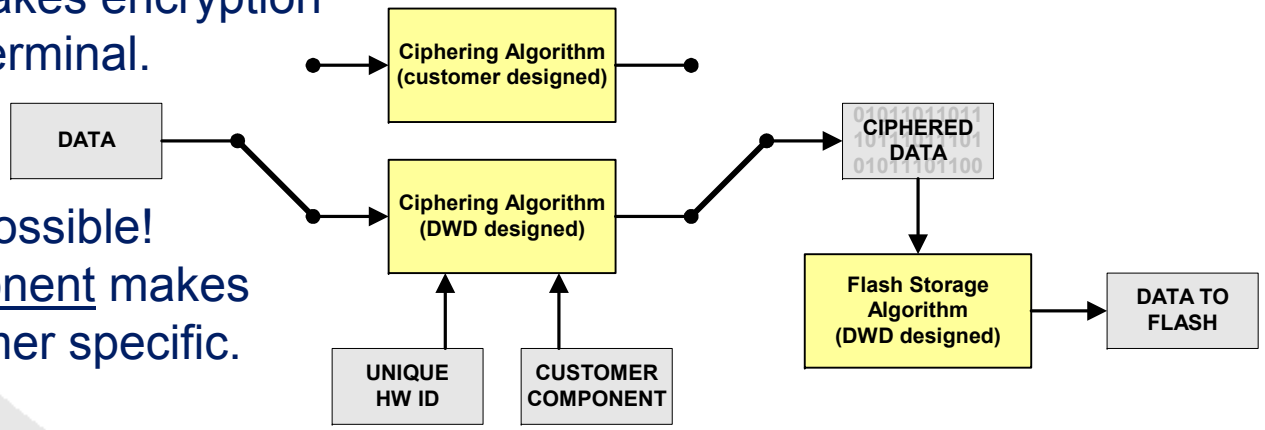
Overview – Customer Delivery

- The Procedure for New Customers
  - DWD is contacted with info about the "Customer" and "Project Name".
  - Special requirements related to Configuration is stated.
  - The Object Code of SEC will be delivered as part of a System Release from DWD.

- The SEC Object is delivered in binary format to keep the concent secure.
  - The source code of SEC is never surrendered to customers.
  - Only the interface towards SEC will be revealed.
  - Only three persons at DWD are authorized to access the source code of SEC.
  - The source code / design documentation of SEC are stored internally using PGP encryption.
  - Moreover, procedures describes how the SEC module must be handled to avoid leaks.

Overview – Encryption and Security

- IMEI and SIM Lock data is encrypted
  - To secure the stored personalization data against fraudulent tampering.
  - The Control Key's (unlock key) are stored using a number of checksums / characteristics.
  - The Codes Groups, States and Retrial Counters are stored in an encrypted format.
  - The basic personalization operations will be encapsulated (control key verifications, data comparison, retrial counter operations etc).
- DWD or Customer Specific Encryption Algorithm
  - Unique HW ID makes encryption unique for each terminal. Flash copy from one ME to another ME not possible!
  - Customer Component makes encryption customer specific.



The security module ensures that a personalized ME stays personalized!

Overview – Standard Solution

- The Overall Functionality Supported:
  - Tool Access Restriction
  - Write IMEI (via Phone Tool)
  - SIM Locks Programming (via Phone Tool)

- Configuration Options:
  - IMEI one time programming or multiple time programming.

- The Standard Solution Delivery includes:
  - SEC.obj: The Security Object binary delivered by DWD.
  - PSC File Editor and Programmer (included in Phone Tool) delivered by DWD.

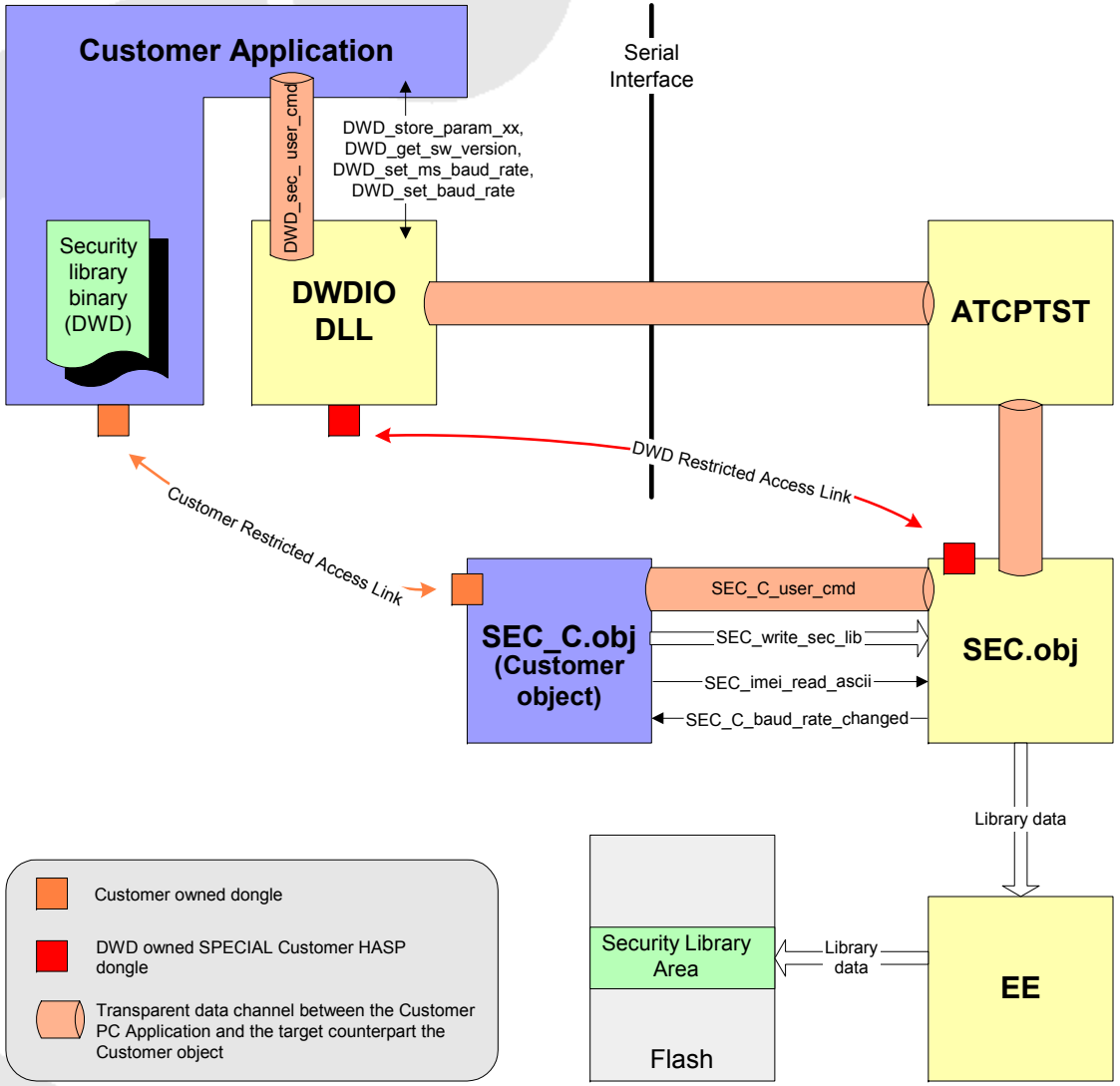
Overview – Sec Library Concept 1

- The Overall Functionality Supported:
  - Tool Access Restriction
  - Write IMEI and Erase SIM Locks programming only possible after restoring Security Library Binary.
  - Restoring Security Library Binary only possible via special link between Customer PC Application and Customer Specific SEC_C object in ME.

- The Security Library Concept SEC Solution Delivery includes:
  - SEC.obj: The Security Object delivered by DWD.
  - Security Library Binary (removable binary code) delivered by DWD.
  - SEC_C.obj: Customer Object delivered by Customer. (DWD provides a template version with source)
  - Customer PC Application delivered by Customer (DWD provides a template version ”SEC Transfer” with source)

Overview – Sec Library Concept 2

- The Security Library Concept includes a customer specific PC Application and customer specific SEC_C Object.
- Using Customer Restricted Access Link the Security Library Binary may be restored in order to enable Write IMEI functionality and Erase SIM Locks functionality.



Overview – The End

QUESTIONS...