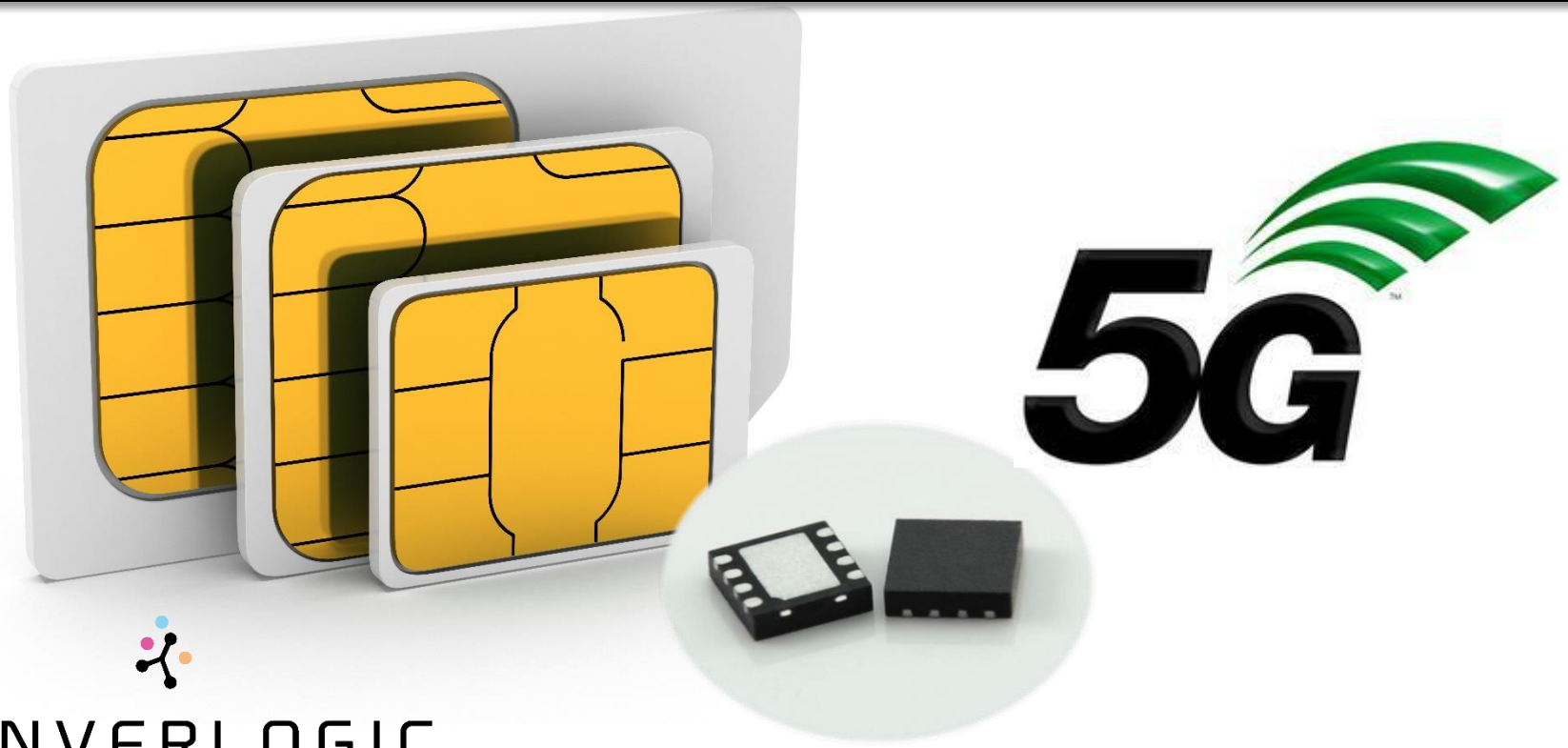
SIM Evolution

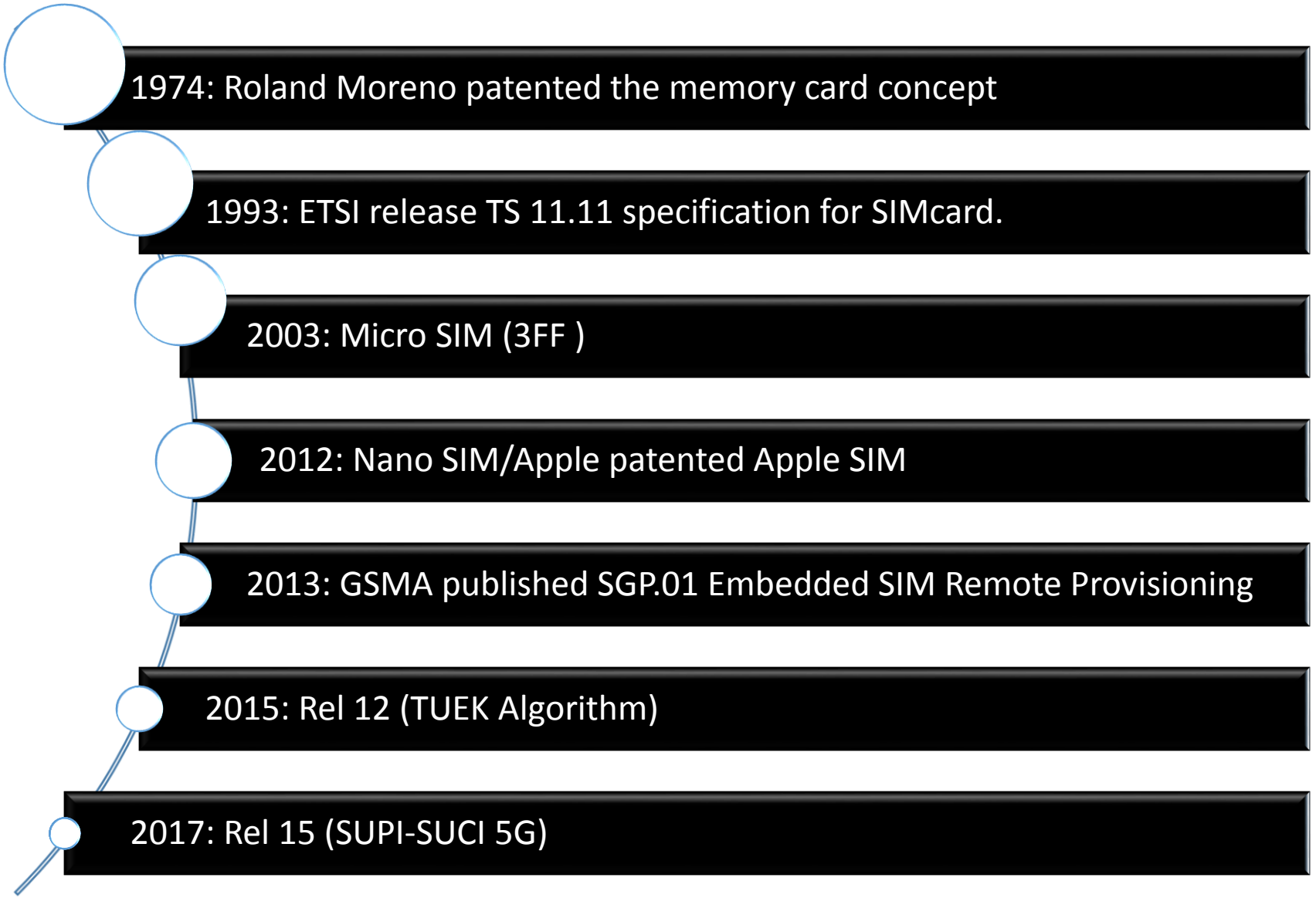


CONVERLOGIC

mobility solutions

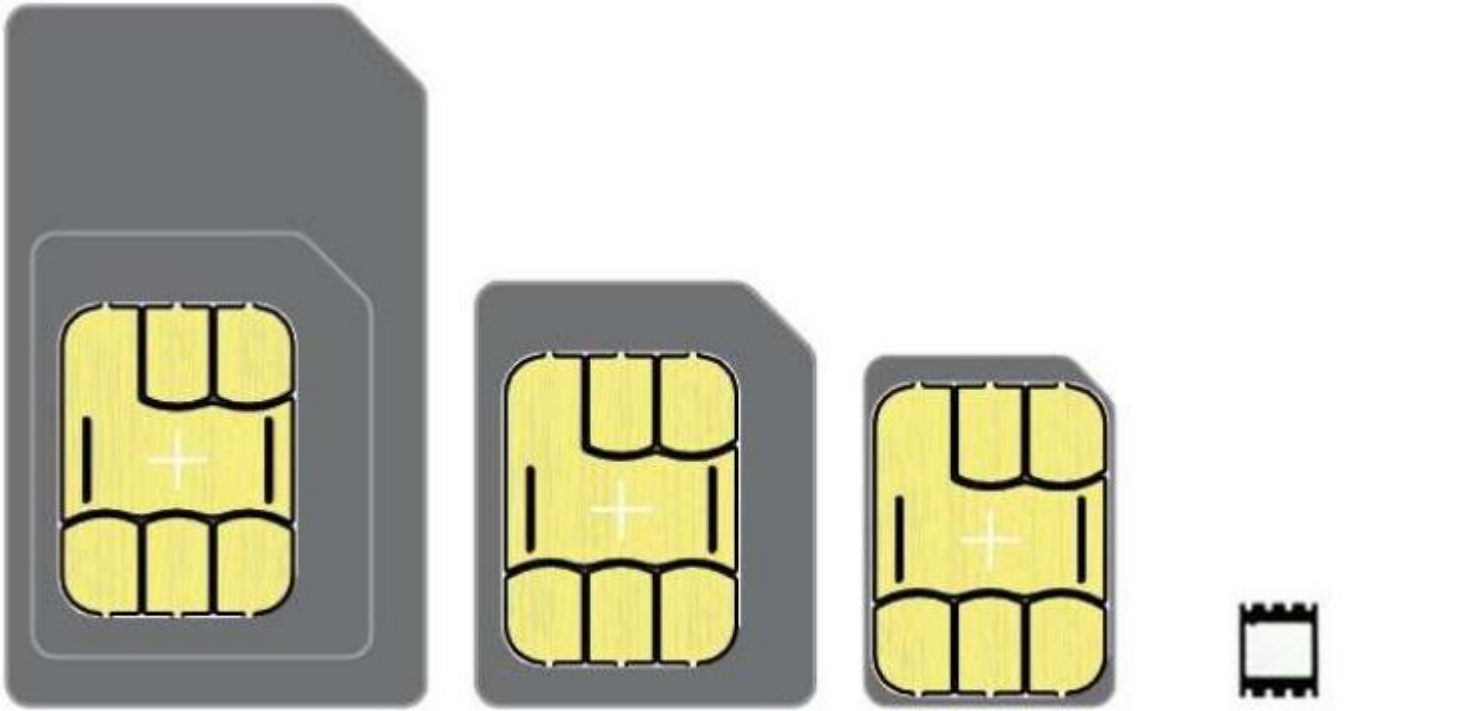
SIM History

CONVERLOGIC
mobility solutions



SIM factors evolution

CONVERLOGIC
mobility solutions



2FF - Mini SIM
25mm x 15mm x 0,76mm

3FF - Micro SIM
15mm x 12mm x 0,76mm

4FF - Nano SIM
12,3mm x 8,8 x 0,67mm

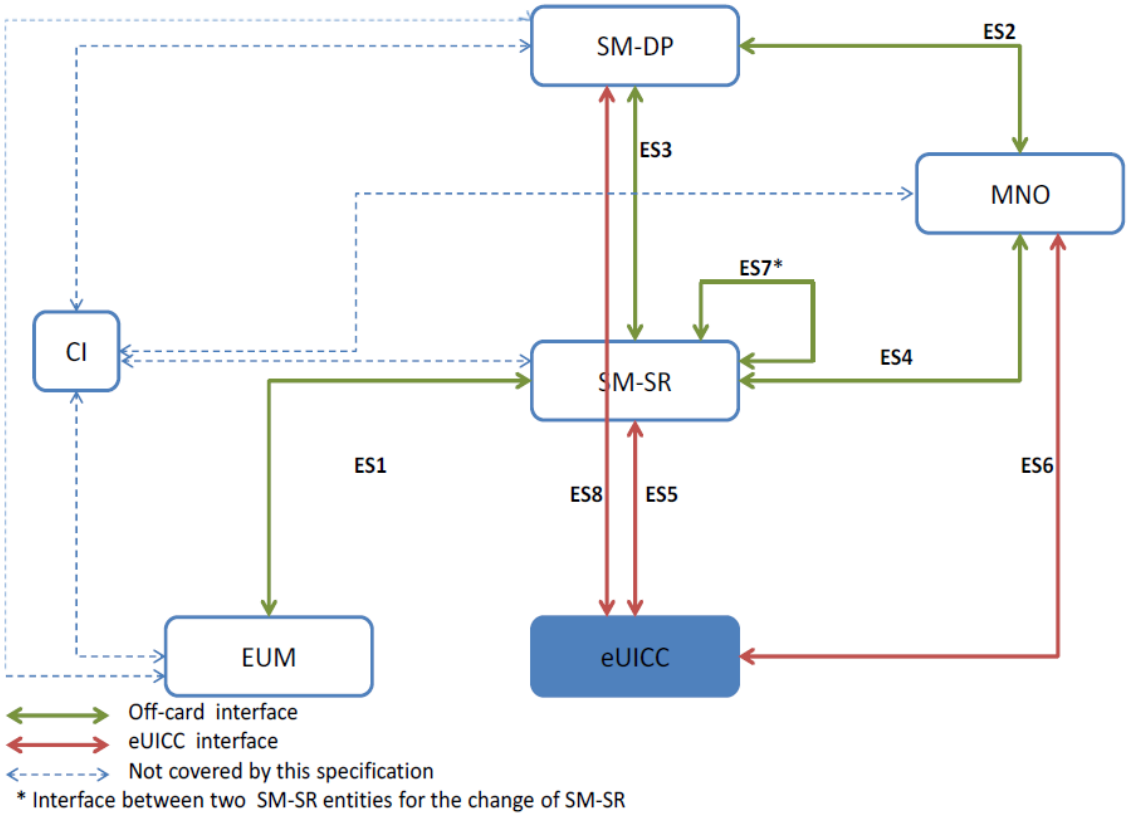
MFF2
M2M Form Factor

M2M Architecture

CONVERLOGIC
mobility solutions

Remote SIM Provisioning for M2M utilises a server driven (push model) to provision and remotely manage operator Profiles.

1. SM-DP (Subscription Manager - Data Preparation)
2. SM-SR (Subscription Manager - Secure Routing)
3. eUICC.



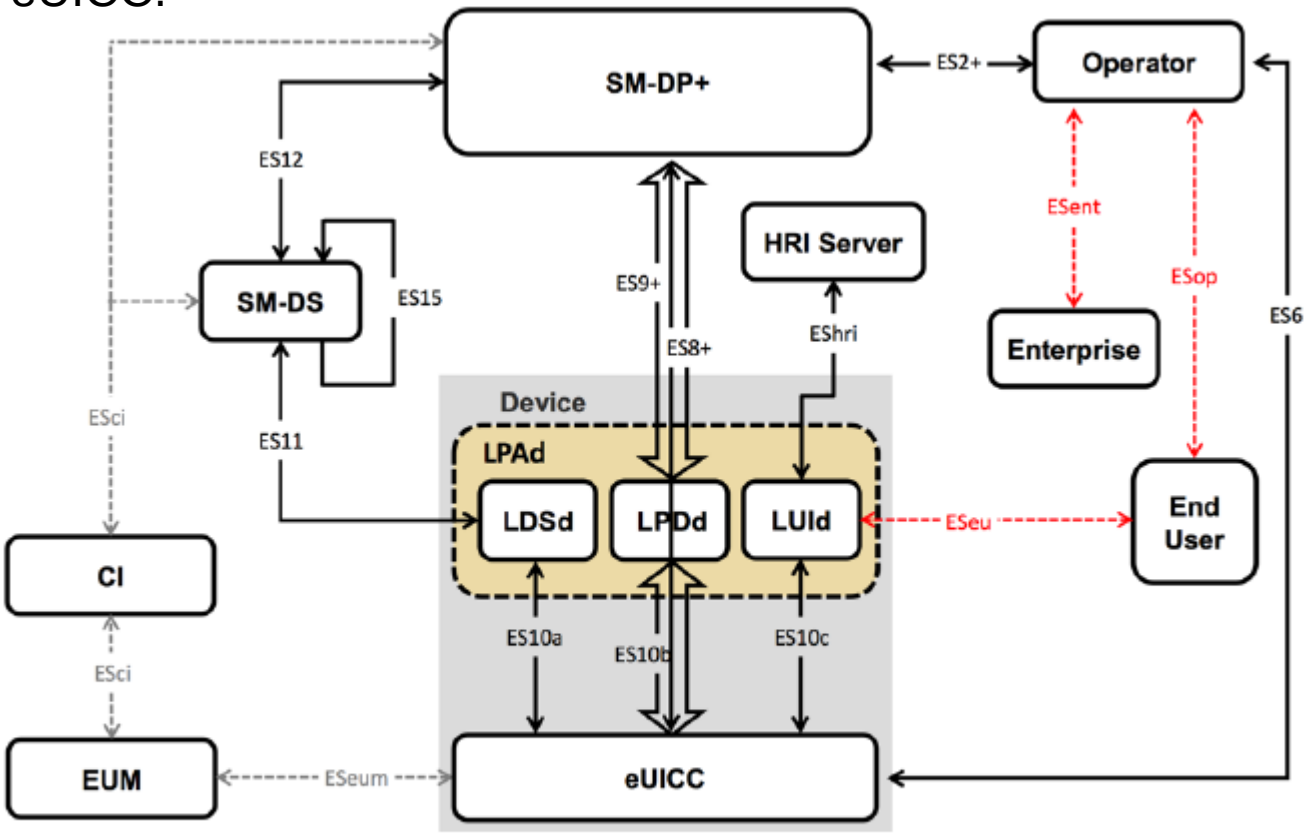
GSMA

Consumer Architecture

CONVERLOGIC
mobility solutions

Remote SIM Provisioning for M2M utilises a server driven (push model) to provision and remotely manage operator Profiles.

1. SM-DP+ (Subscription Manager - Data Preparation)
2. SM-SR (Subscription Manager - Secure Routing)
3. LPA + eUICC.



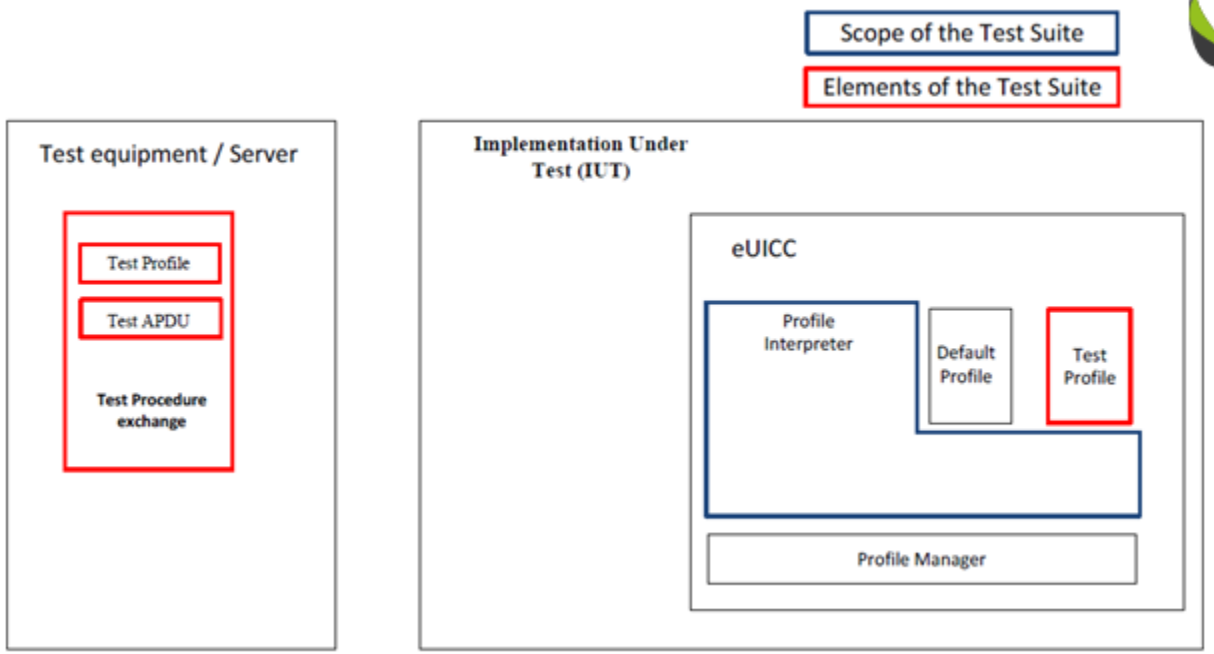
Remote SIM Provisioning for Consumer Architecture

eSIM format files

CONVERLOGIC
mobility solutions

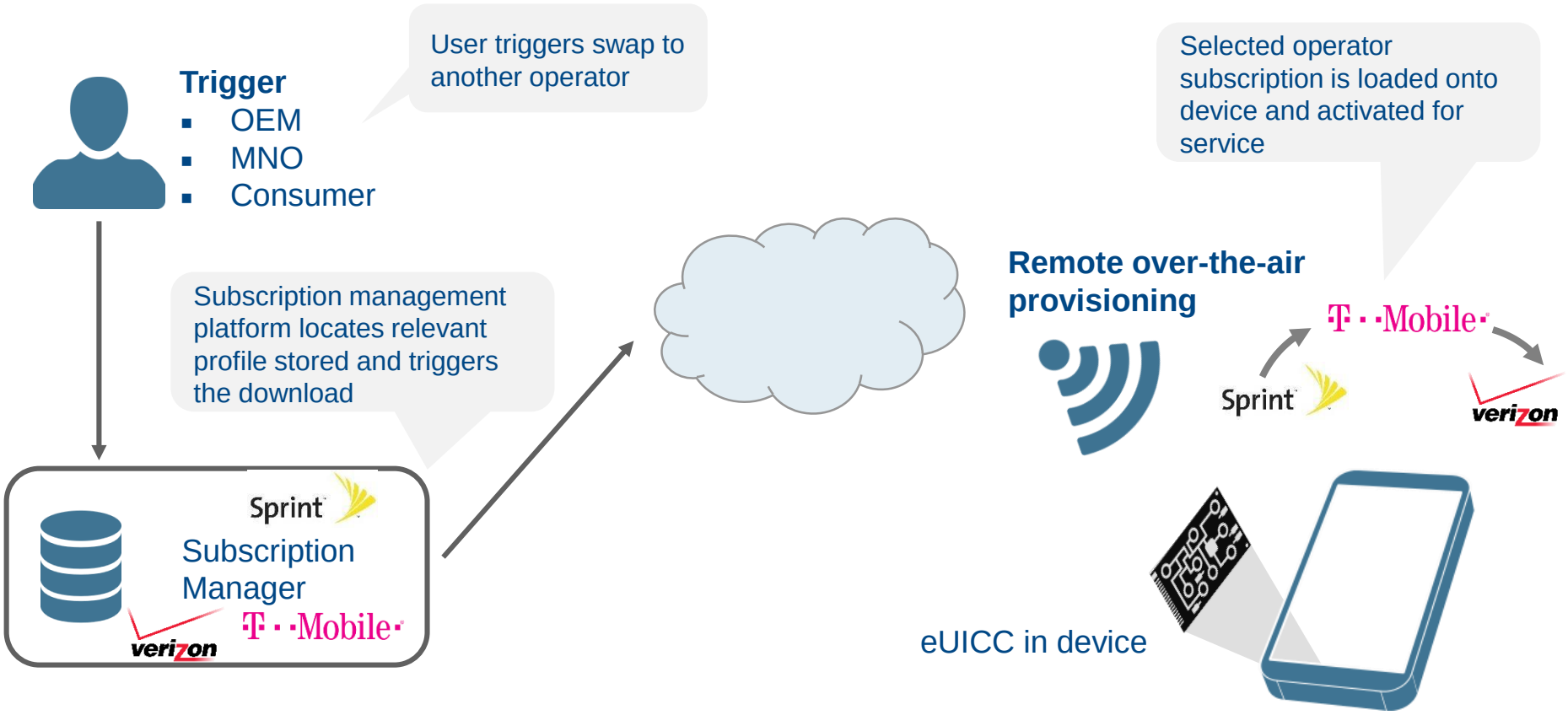
SIMalliance had managed This document defines the technical specification of a standard format to be used for the loading and installation of an interoperable Profile Package in any compliant eUICC. This specification is based on the following SIMalliance document: eUICC Profile Package: Interoperability Functional Requirements.

simalliance



eSIM setup process

CONVERLOGIC
mobility solutions



Source: Arthur D. Little analysis, GSMA eUICC specification v3

SIM/eSIM Market

CONVERLOGIC
mobility solutions

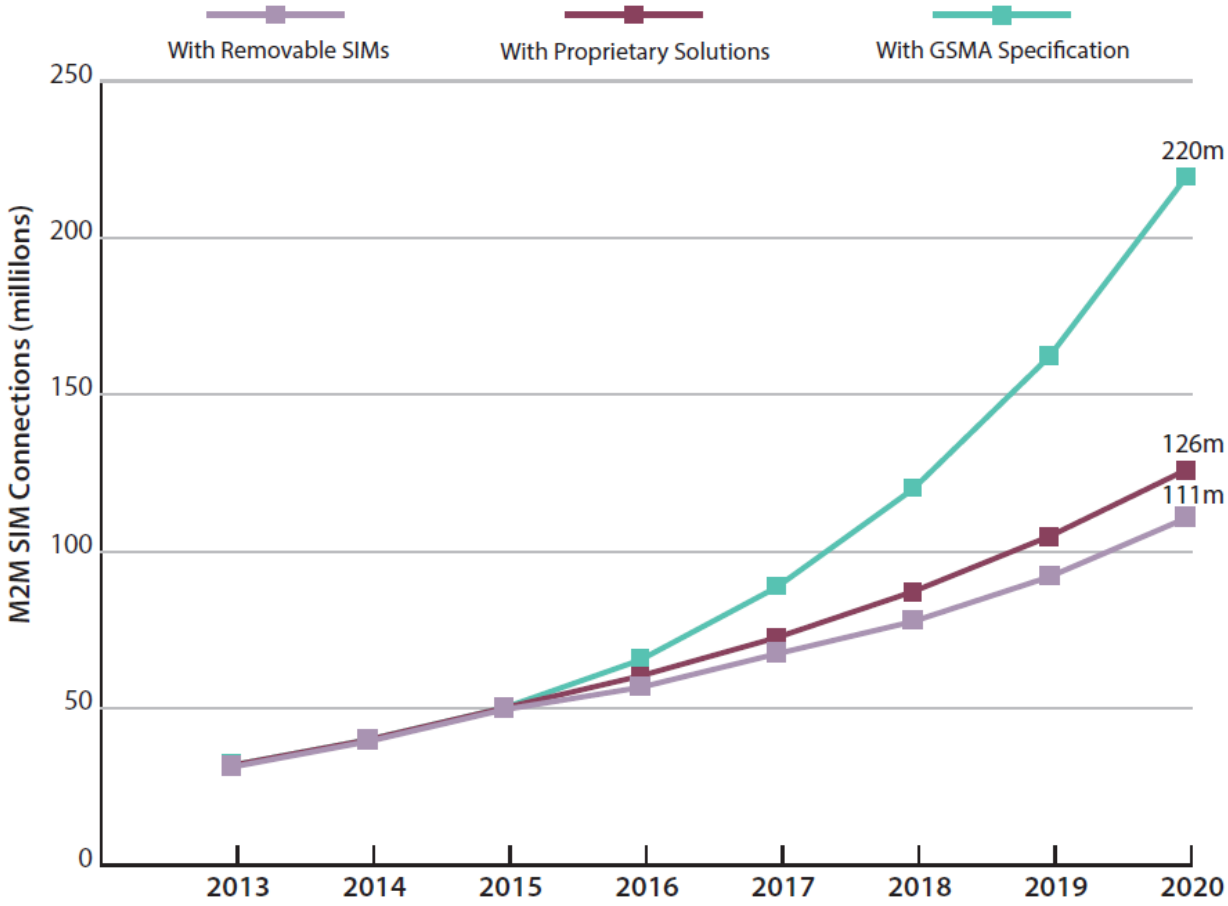


Figure 1.3: Projected Consumer Electronics Connections worldwide with alternative scenarios

SIM/eSIM Market

CONVERLOGIC
mobility solutions

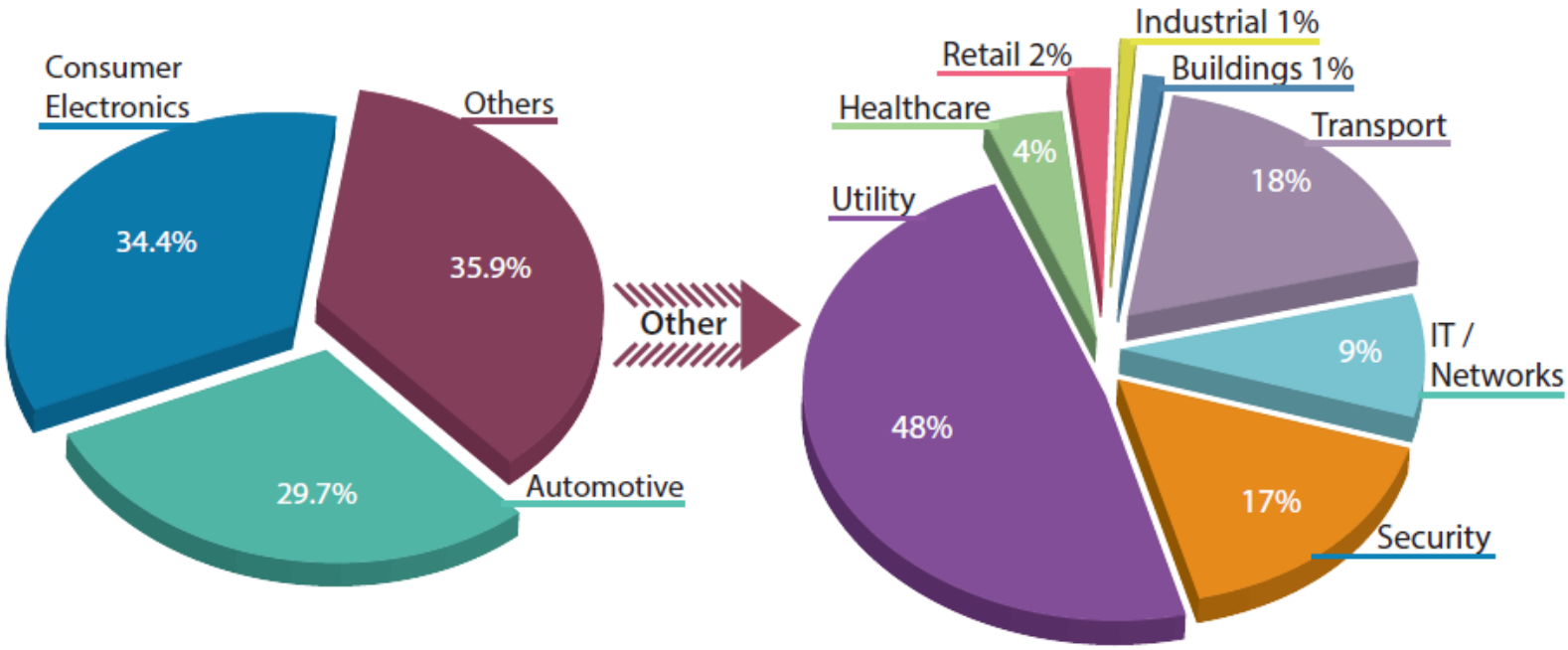
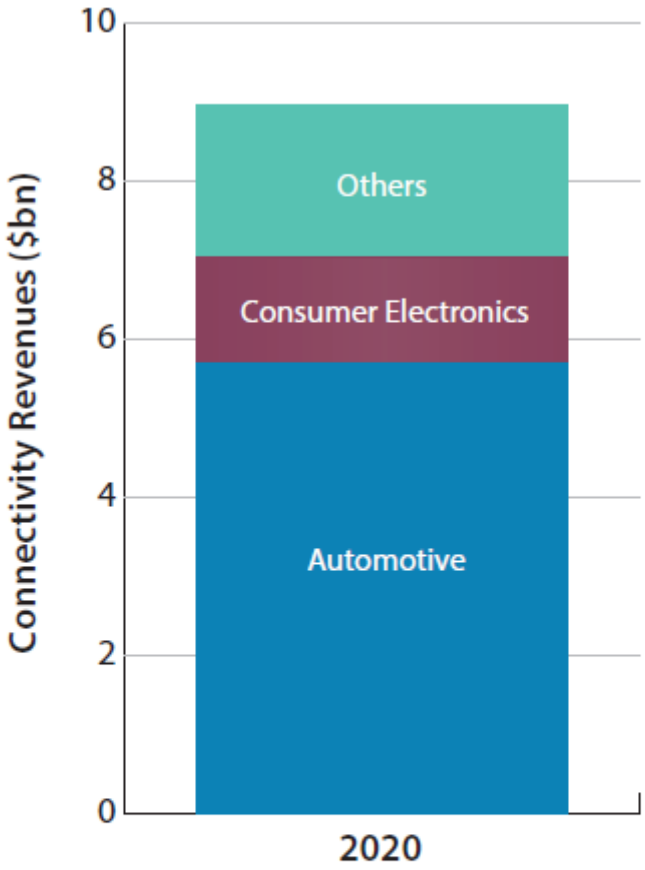


Figure 1.4: Breakdown of M2M Connections per Sector in 2020 in the Case of GSMA Embedded SIM Specification

SIM/eSIM Market

CONVERLOGIC
mobility solutions



Connectivity Revenues	($bn)
Automotive	5.70
Consumer Electronics	1.33
Others	1.93
Total	8.96

eSIM Wareables

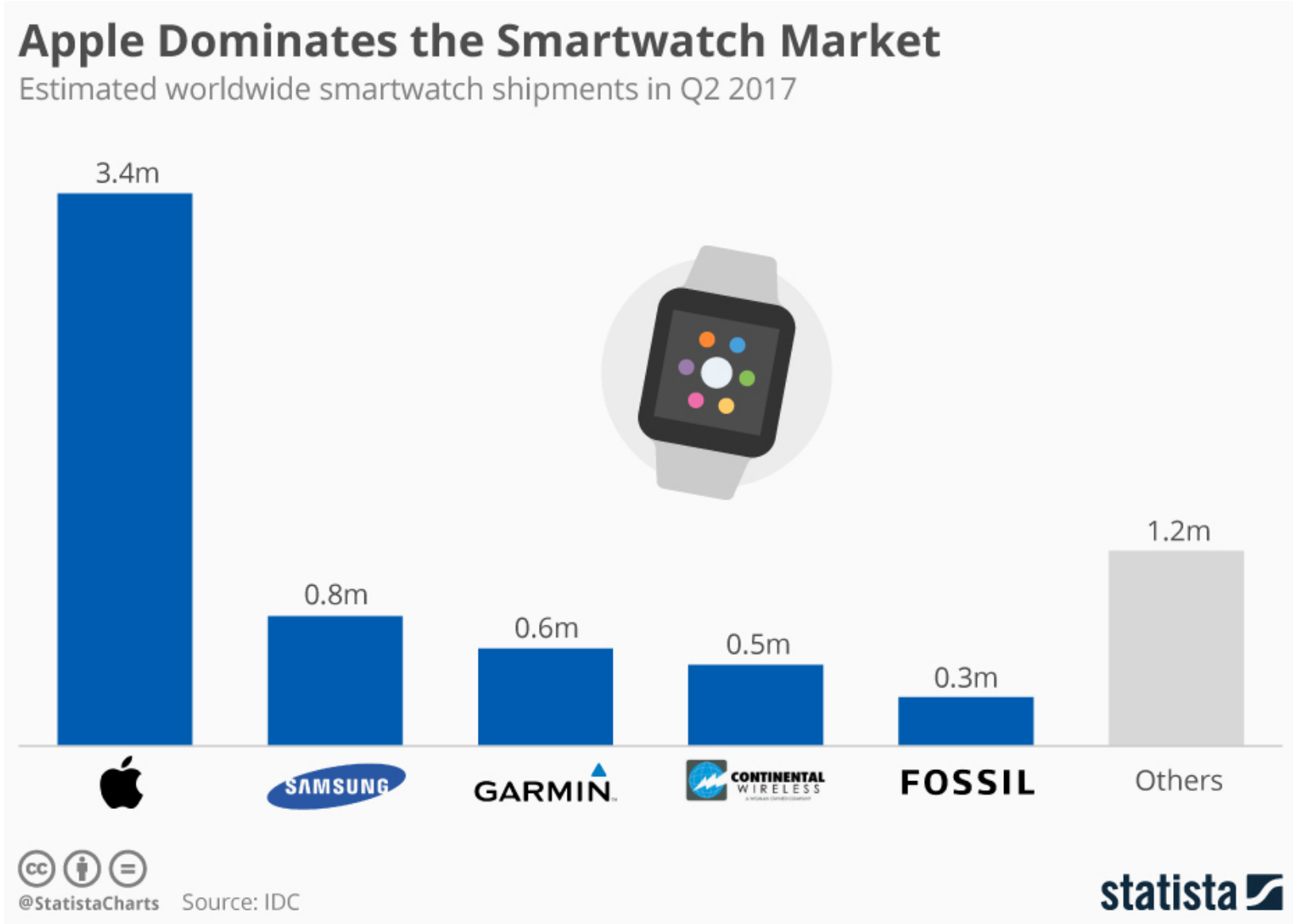
CONVERLOGIC
mobility solutions

CHALLENGES OF **WEARABLE DEPLOYMENTS**

	Security Challenges				*Logistical Challenges*				
eUICC features / functionality	Privacy breaches	Data tampering	Software / firmware integrity	Lost & stolen devices	Standalone connectivity	Subscription mgmt	Device miniaturisation	Hostile environment	Battery life
Remote provisioning & mgmt	✘	✘	✘	✘		✘			
Tamper resistant	✘	✘	✘	✘					
Isolated	✘	✘	✘	✘					
Encryption	✘	✘	✘	✘					
GSMA certified	✘	✘	✘		✘	✘			
Multiple connectivity profiles					✘	✘			
Soldered		✘		✘			✘	✘	
Miniaturised							✘	✘	
Ruggedised								✘	
Low power									✘

eSIM Wareables

CONVERLOGIC
mobility solutions



SIM 5G

CONVERLOGIC
mobility solutions

5G SIM: a tamper-proof secure element which is the only solution allowed to secure 5G network access.

specified by the 5G standardization body ETSI-3GPP in Release 15

- ✓ User privacy management
- ✓ Mobile security architecture
- ✓ 5G roaming
- ✓ Extended battery life
- ✓ Quality of Experience



5G (from release 12 to 15)

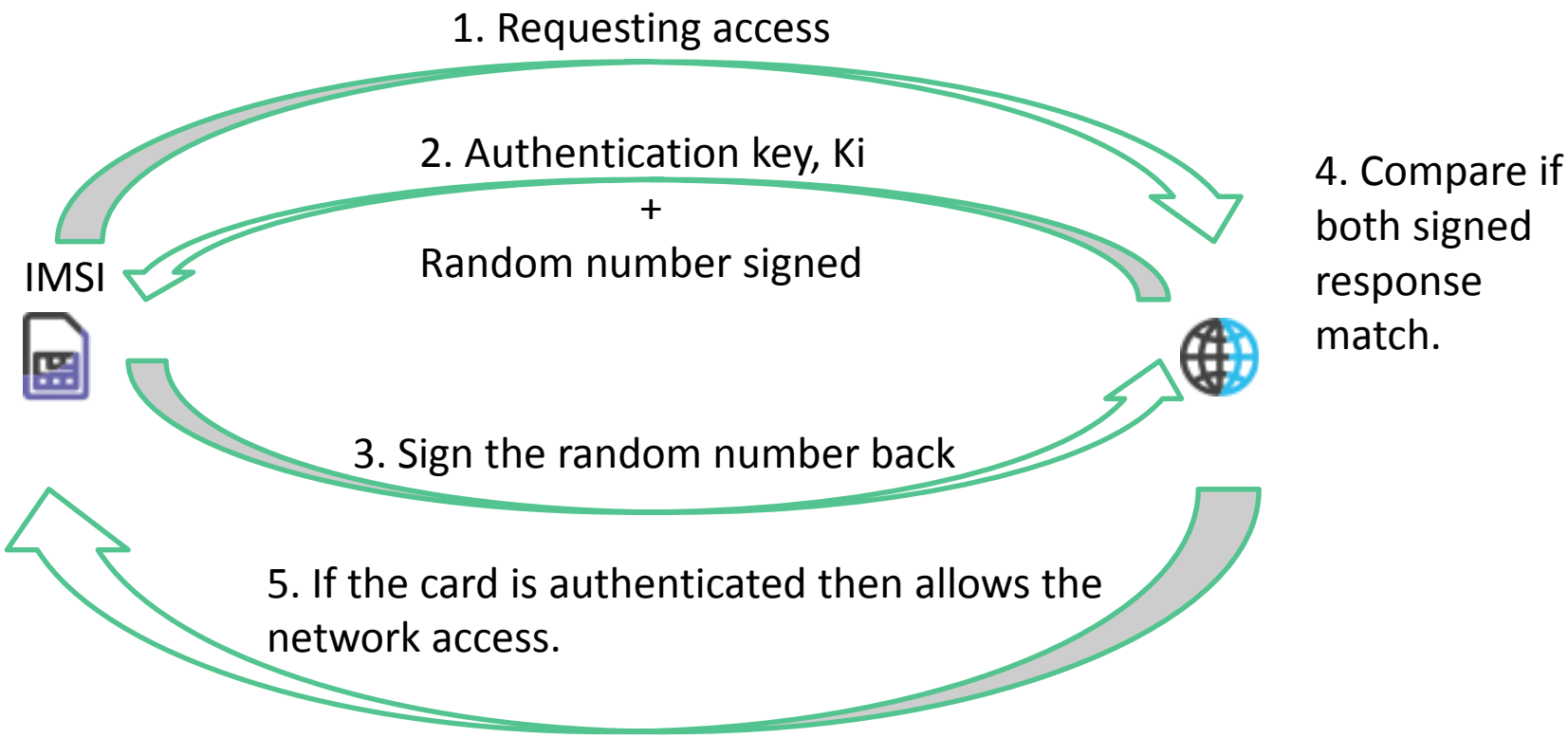
CONVERLOGIC
mobility solutions

- **ETSI TS 122 261:** 5G; Service requirements for next generation new services and markets
- **ETSI TS 133 501:** 5G; Security architecture and procedures for 5G System **(SUCI calculation)**
- **ETSI TS 123 501:** System Architecture for the 5G System
- **ETSI TS 123 502:** Procedures for the 5G System

5G Authentication Process

CONVERLOGIC
mobility solutions

Milenage-> TUAK (rel 12)



5G Protecting privacy

CONVERLOGIC
mobility solutions

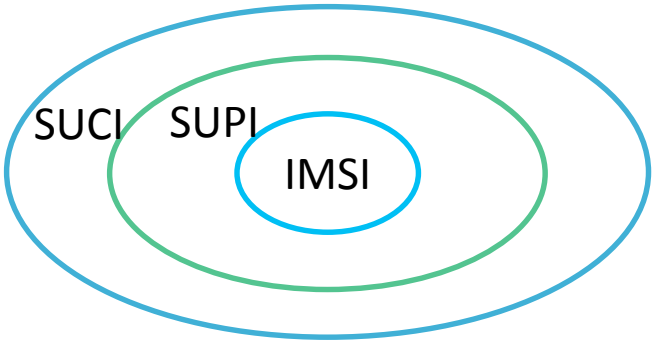
subscriber privacy: IMSI privacy

IMSI: International Mobile Subscriber Identity



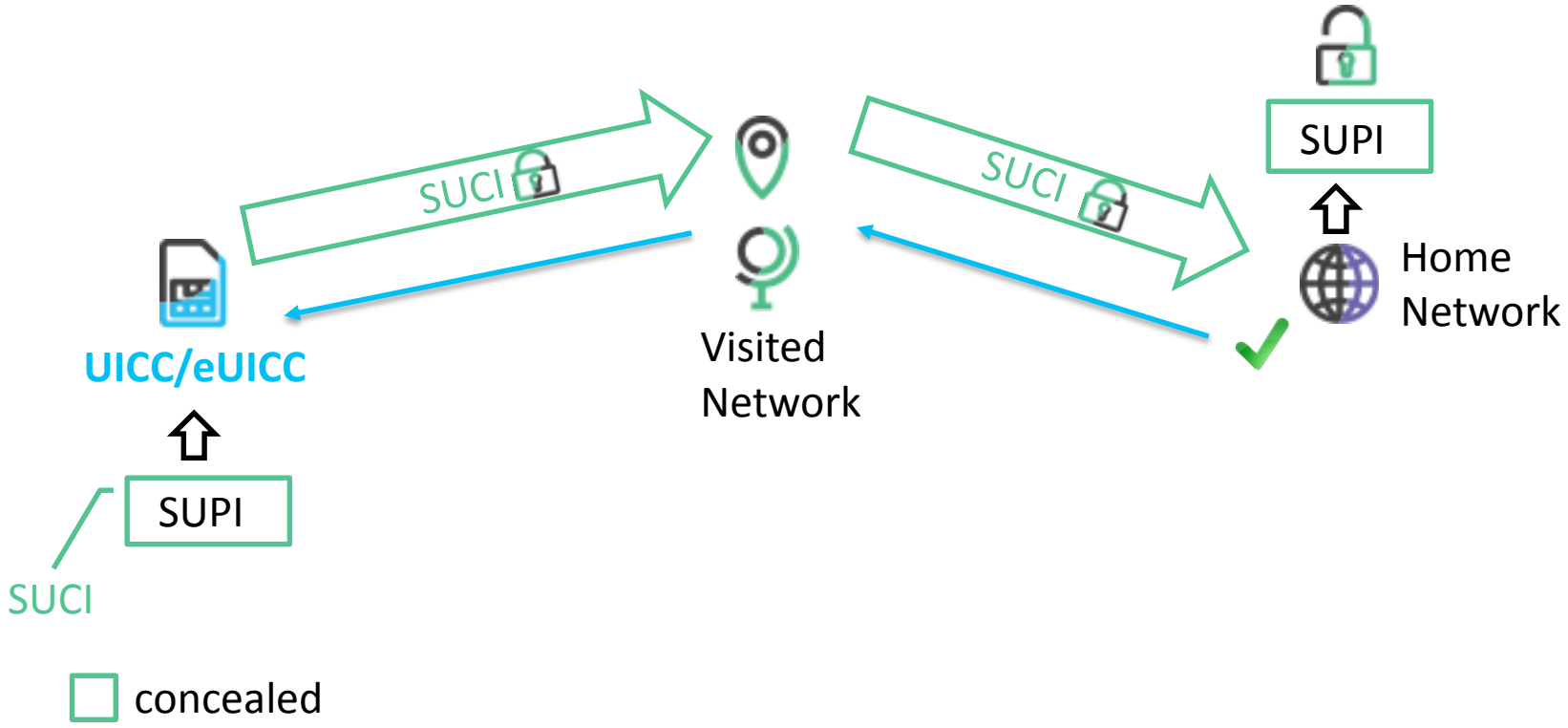
- Unique for each mobile device
- Allow the authentication in the network
- It is integrated into the UICC

- Storing MNO public key
- It is contained by the SUPI
- SUPI is concealed by the SUCI
- SUCI encryption within the SIM



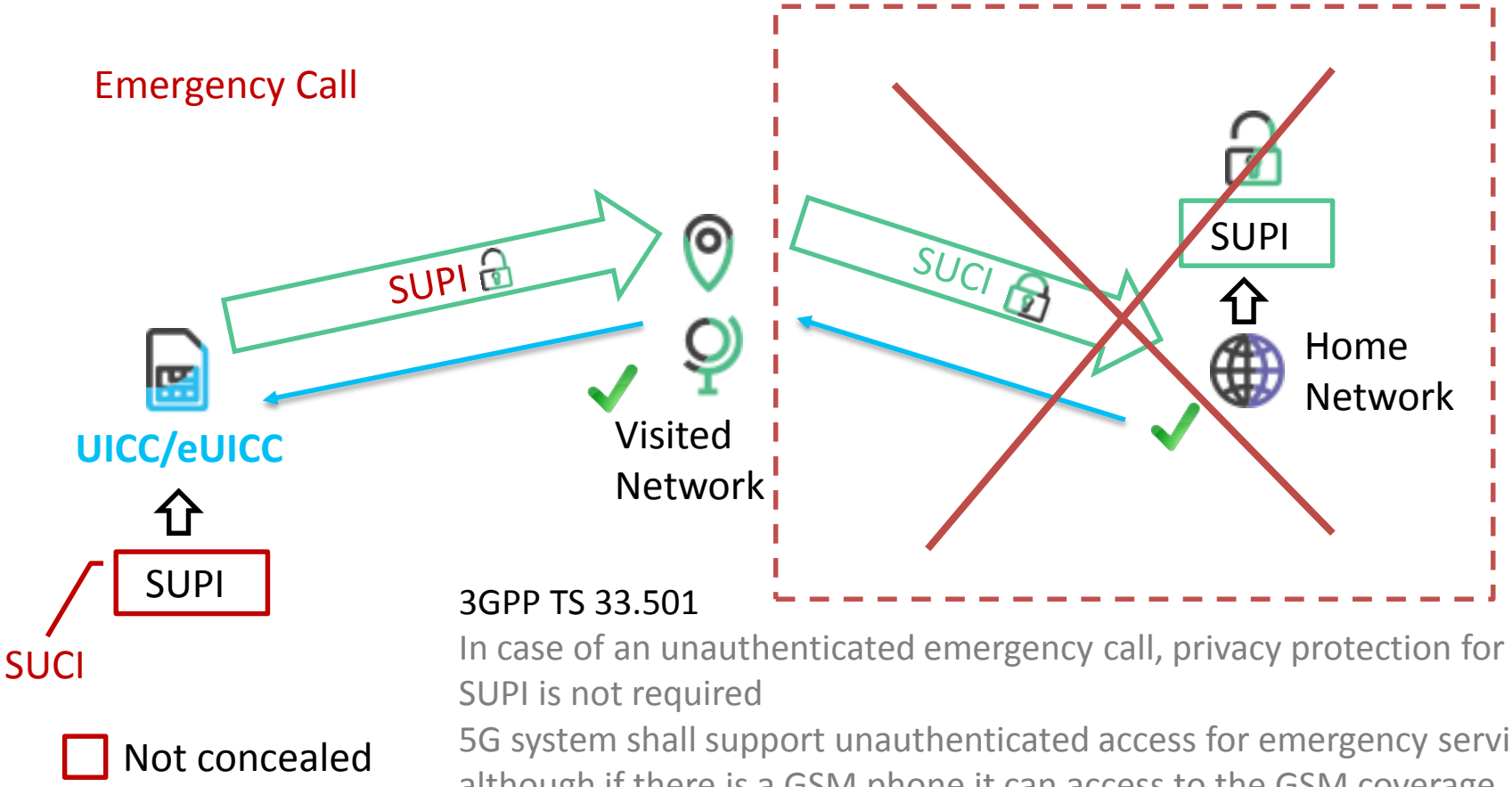
5G SUPI-SUCI

CONVERLOGIC
mobility solutions



5G SUPI-SUCI

CONVERLOGIC
mobility solutions



3GPP TS 33.501

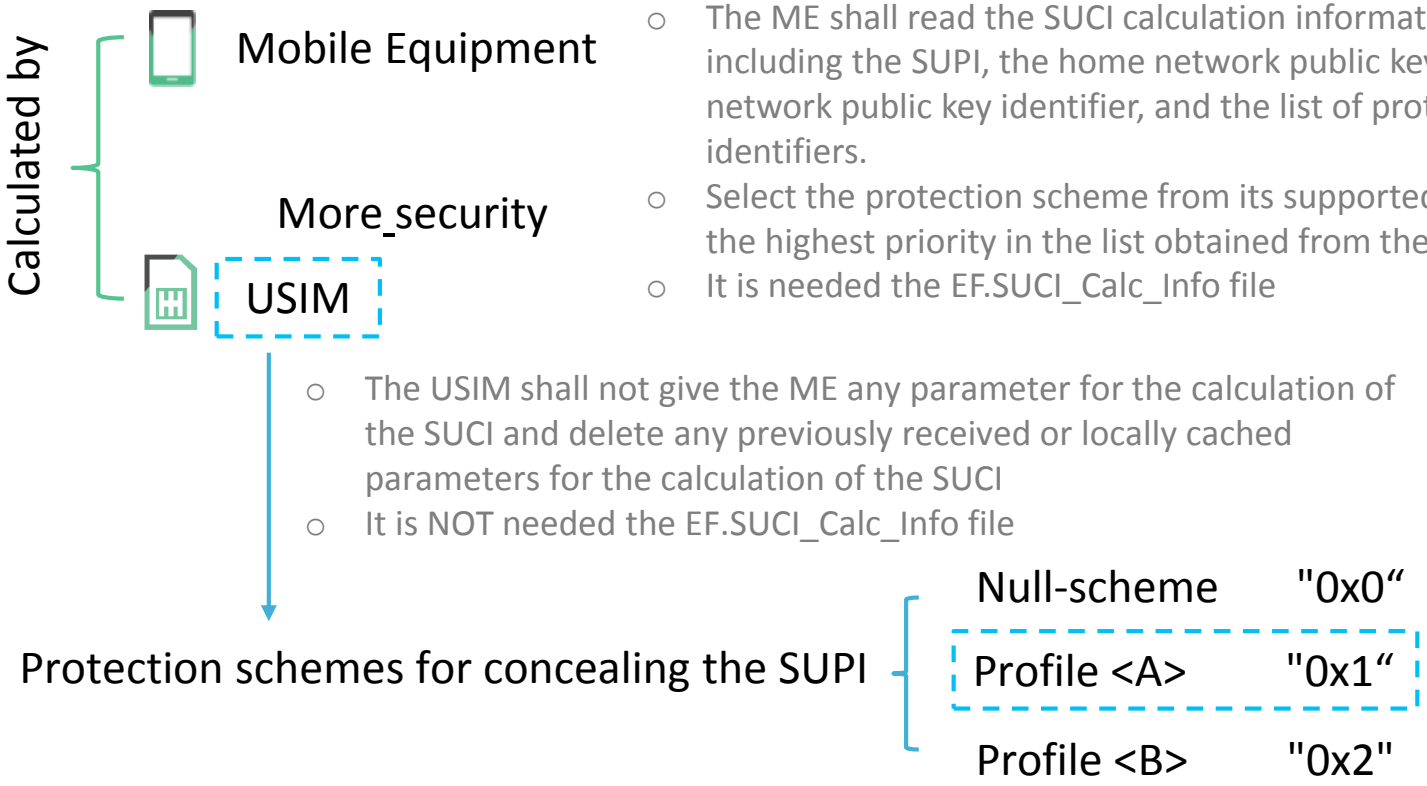
In case of an unauthenticated emergency call, privacy protection for SUPI is not required

5G system shall support unauthenticated access for emergency services although if there is a GSM phone it can access to the GSM coverage without a SIM card

5G SUCI

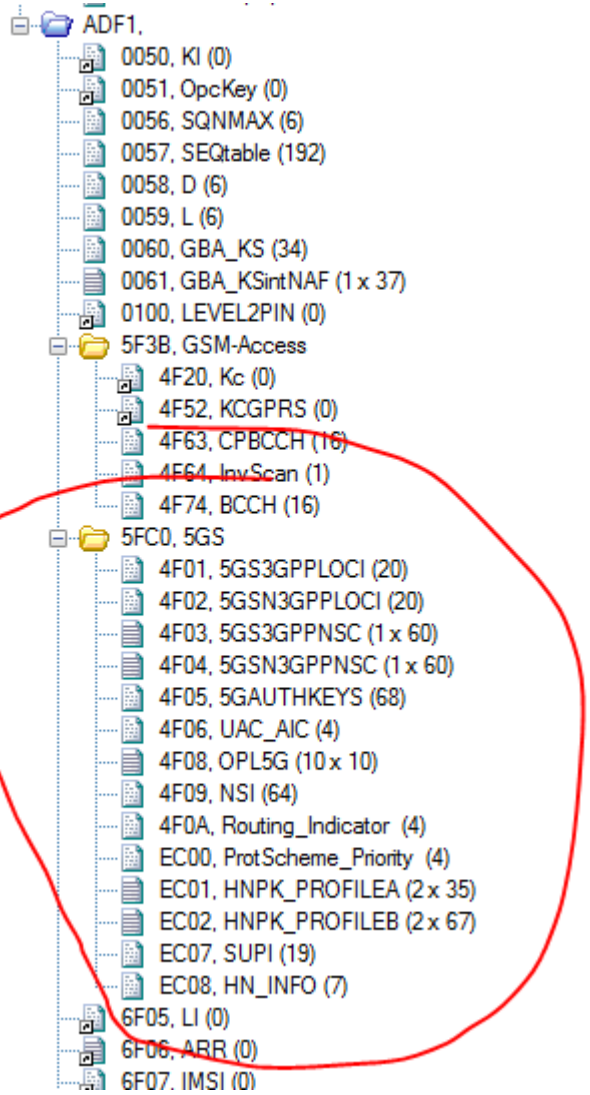
CONVERLOGIC
mobility solutions

One-time use subscription identifier, called The SUbscription Concealed Identifier, which contains the concealed subscription identifier, SUPI.



5G New Files

CONVERLOGIC
mobility solutions

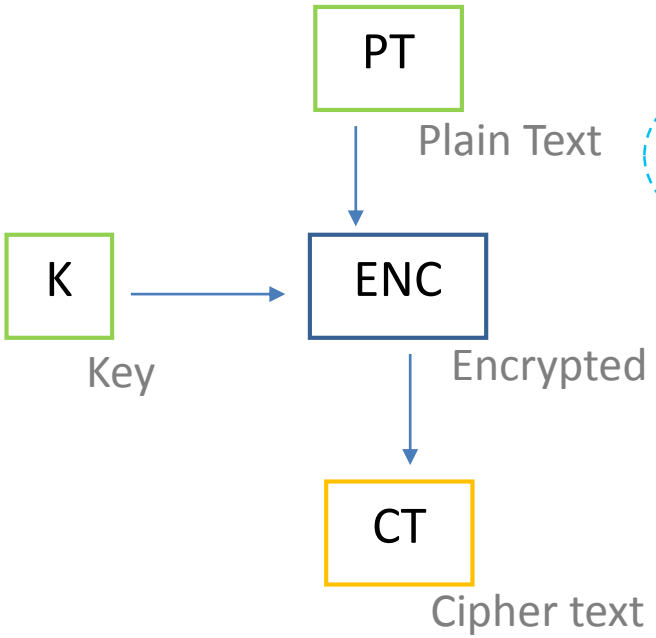


- EF.PLMNwAcT, EF.OPLMNwAcT, EF.HPLMNwAcT: new access technologies
- EF.AD: new specific facilities
- EF.EARFCNList added
- DF.5GS added
- EF.5GS3GPPLOCI added
- EF.5GSN3GPPLOCI added
- EF.5GS3GPPNSC added
- EF.5GSN3GPPNSC added
- EF.5GAUTHKEYS added
- EF.UAC_AIC added
- EF.SUCI_Calc_Info (for SUCI calculated by the ME)
- EF.Steering_of_UE_in_VPLMN added
- EF.UST: new services (Rel 13, Rel 14, Rel 15)
- EF.NASCONFIG: new TLVs included in content (Rel 13, Rel 14, Rel 15)

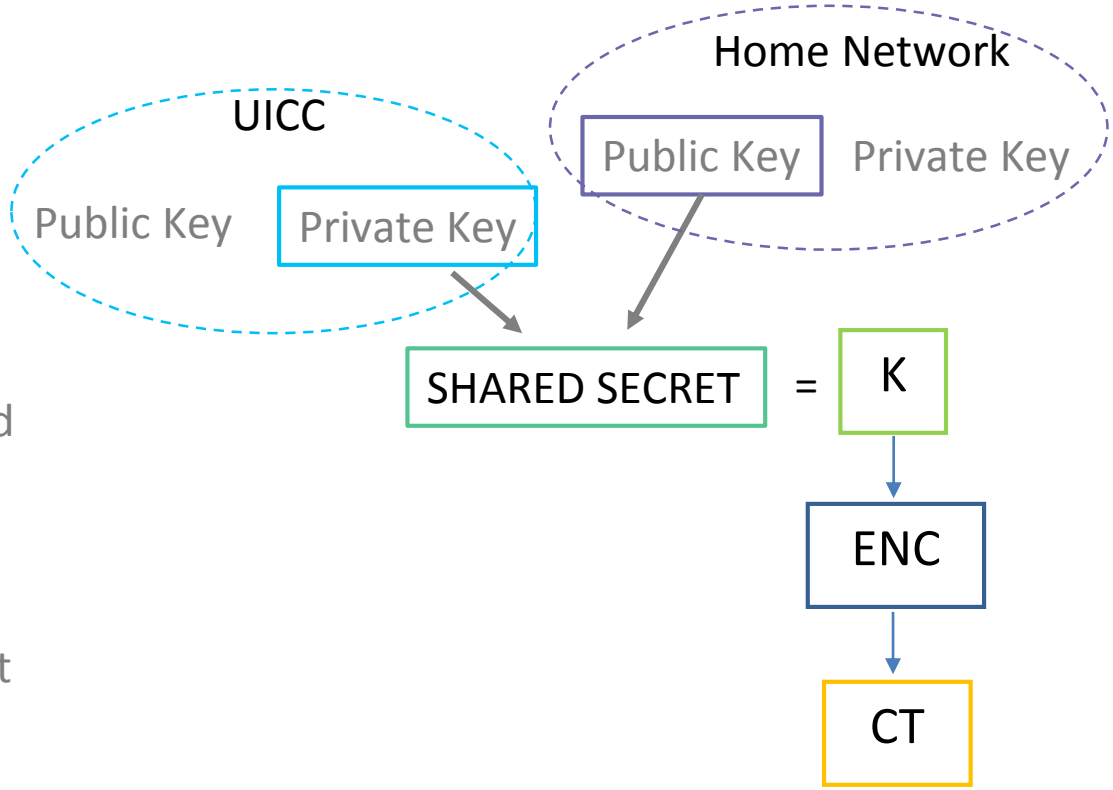
5G How calculate SUCI?

CONVERLOGIC
mobility solutions

Symmetric encryption

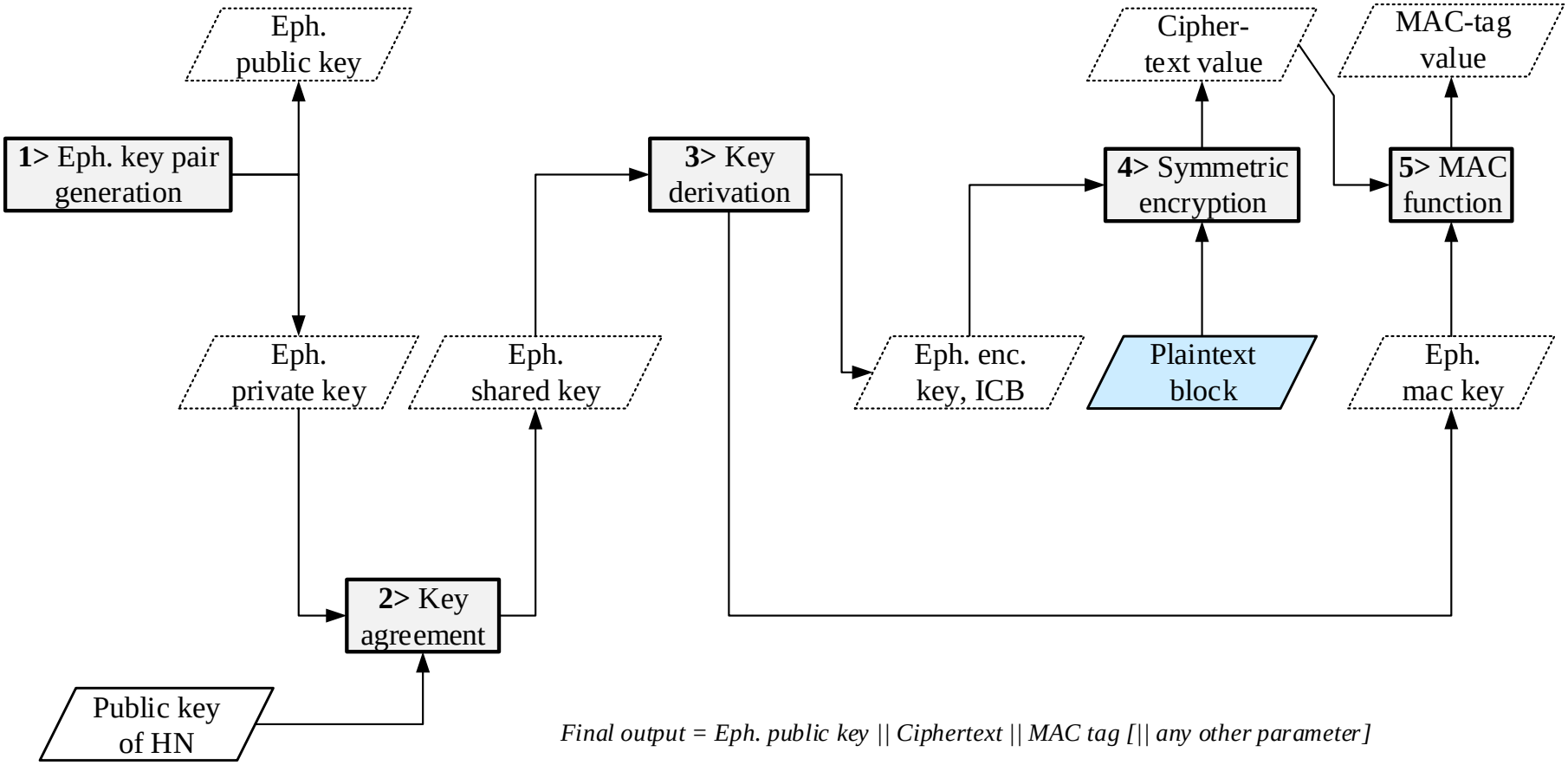


Asymmetric encryption Key agreement



5G How calculate SUCI?

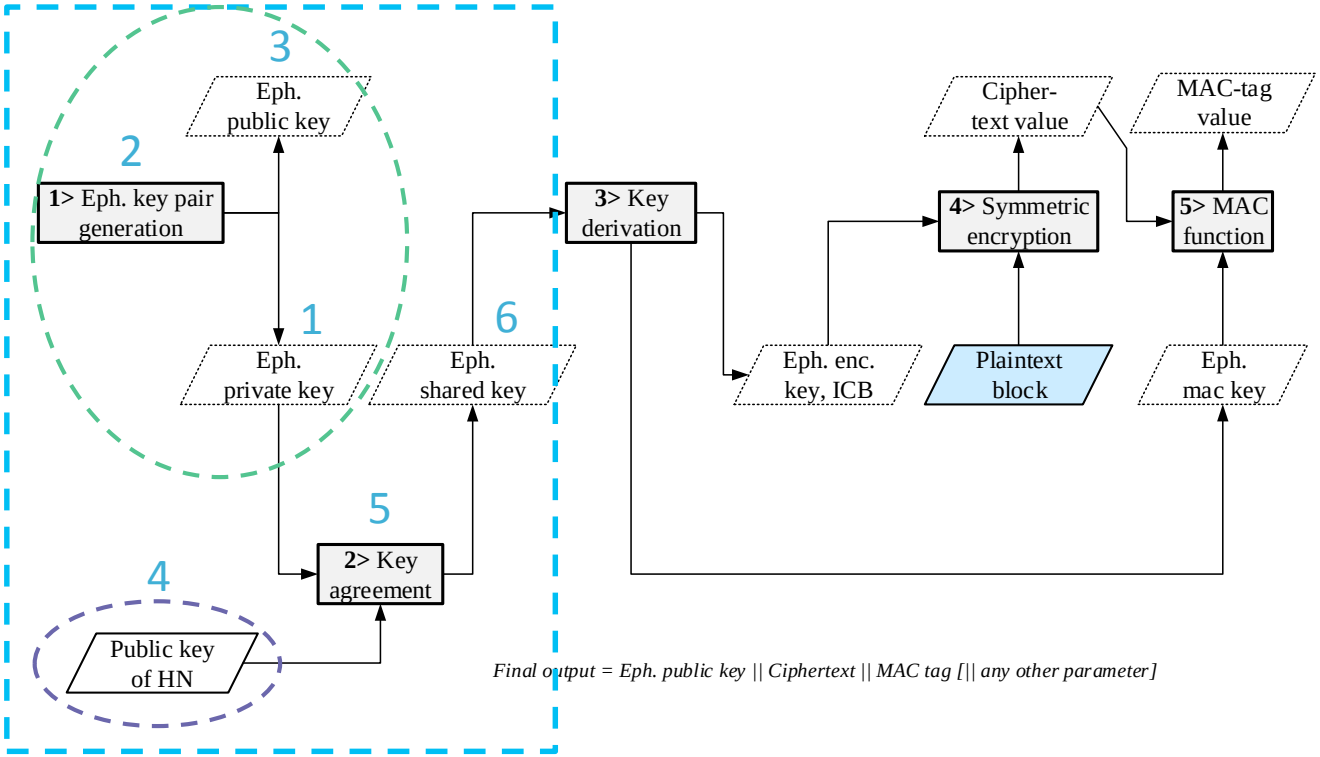
CONVERLOGIC
mobility solutions



Final output = Eph. public key || Ciphertext || MAC tag [|| any other parameter]

5G How calculate SUCI?

CONVERLOGIC
mobility solutions



Starts with the GET IDENTITY command

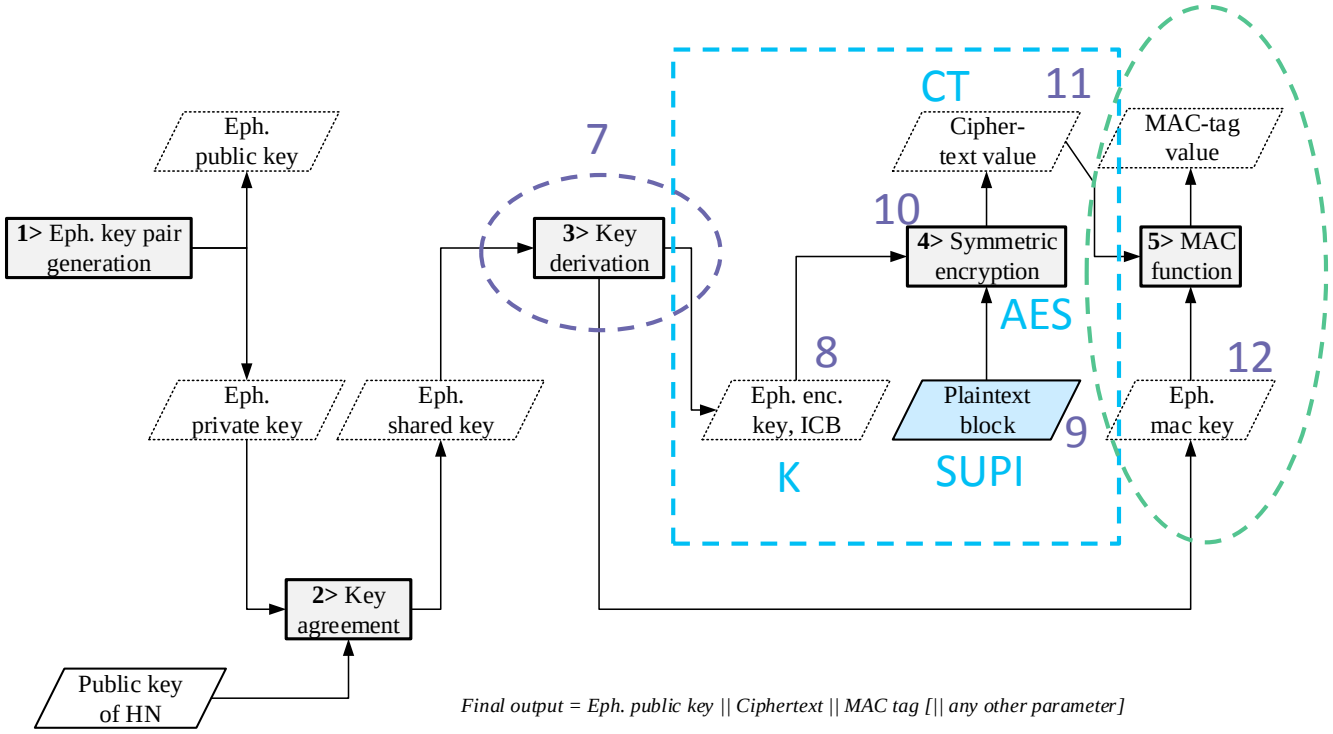
Asymmetric key cryptography 4 Keys, 2 publics and 2 privates

Card Keys

Home Network Keys

5G How calculate SUCI?

CONVERLOGIC
mobility solutions



Symmetric-key cryptography
Same K, just one

Key derivation
create a longer number inserting numbers between

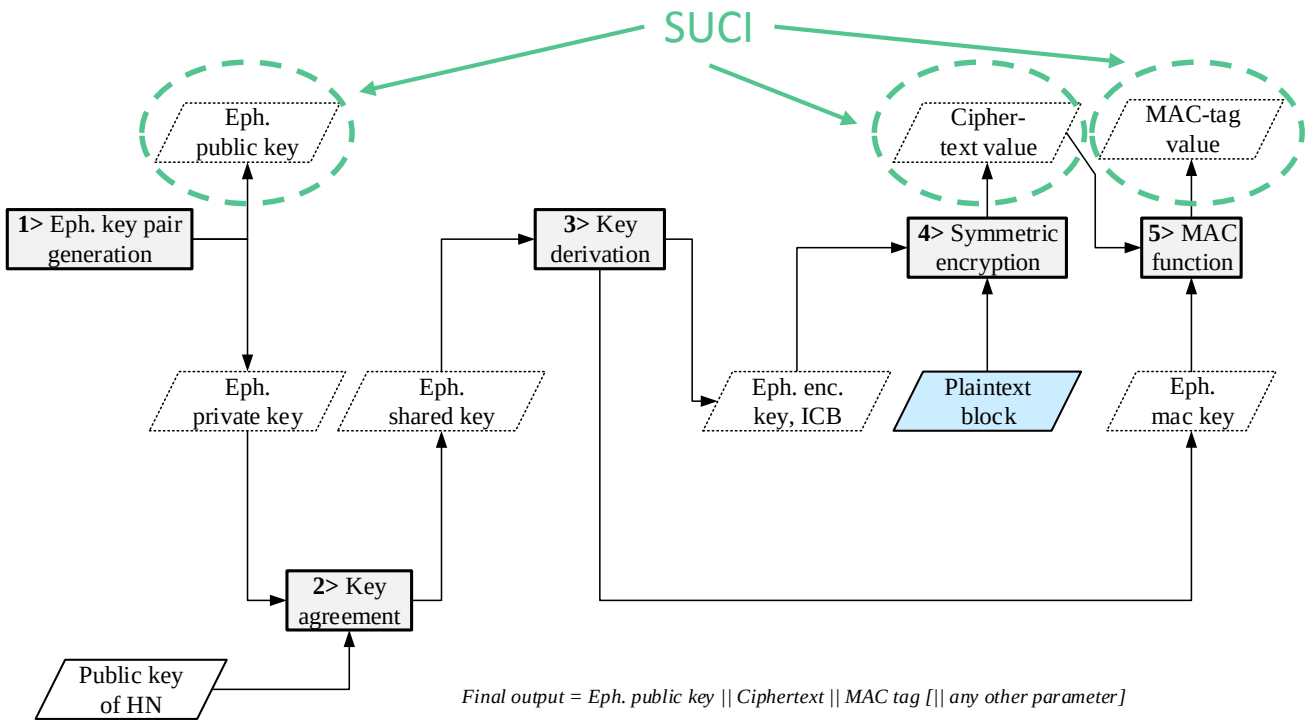
MAC
For calculating the integrity

CT SUPI concealed

5G How calculate SUCI?

CONVERLOGIC
mobility solutions

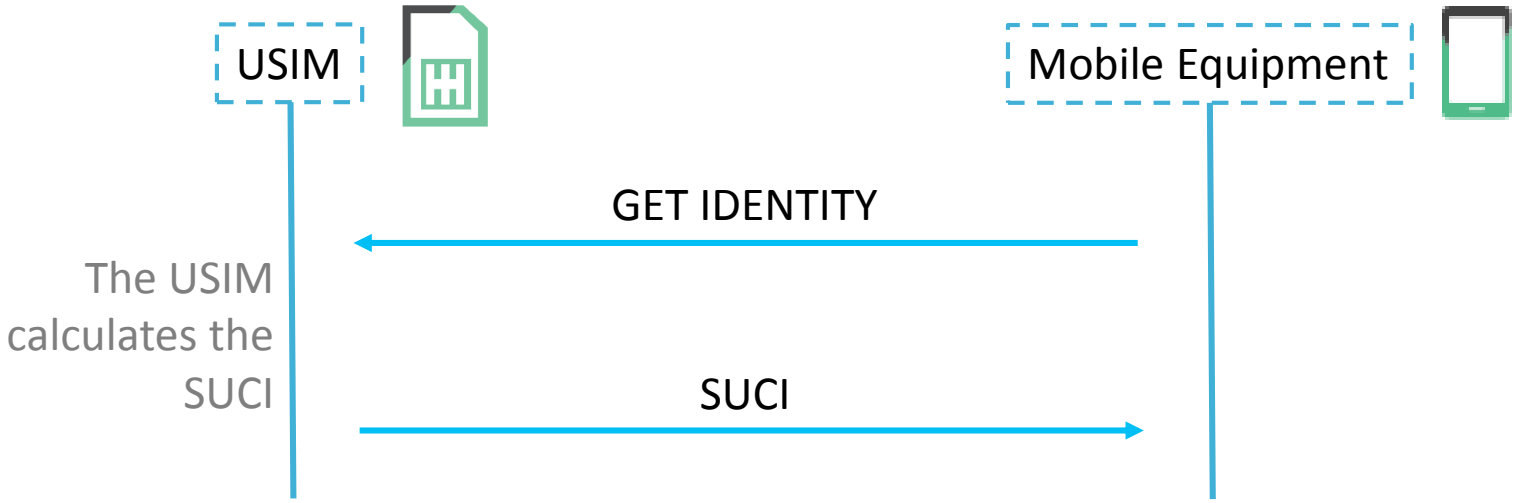
SUCI = Public Key fron the card + CT: SUPI concealed + MAC tag



5G New SIM commands

CONVERLOGIC
mobility solutions

GET IDENTITY



- New command added (ETSI TS 102 221)

THANK YOU!

Jose-Luis Horna

https://download.converlogic.com/eSIM_5G_SIM_Evolution.pdf

Miami Offices:

3045 NW 82nd Ave, Doral FL 33122
United States of America
PH +1 (786) 623-4747
PH +1 (786) 623-4748

jl.horna@converlogic.com

Paris Offices:

12 Rue Sylvain Vigneras
Garches, France 92380
PH +33 (0)1.70.61.75.71