Security Evolution of SIM card

Ravishankar Borgaonkar
ravii@sec.t-labs.tu-berlin.de

TelcoSecDay, Troopers 2014

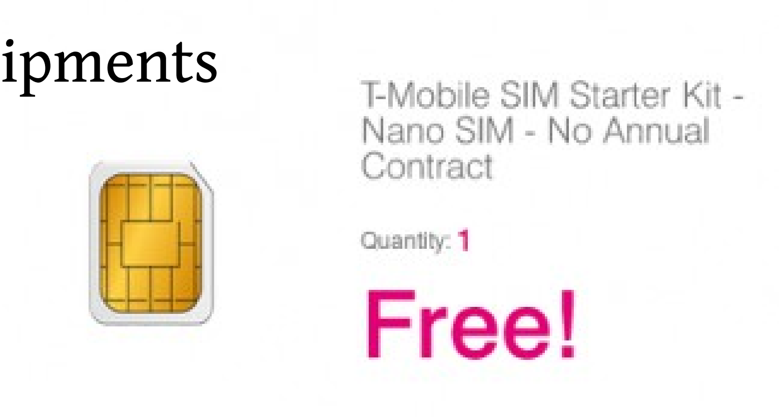
18 March, 2014 – Heidelberg

Overview

- SIM Security and business
- Security and privacy in SIM
- Introduction to new security standard
- Who? What? How ?

SIM cards

- Carrier's money card
- A chip to connect telephony equipments
- Store information and tools
- Provide security
- Add on services

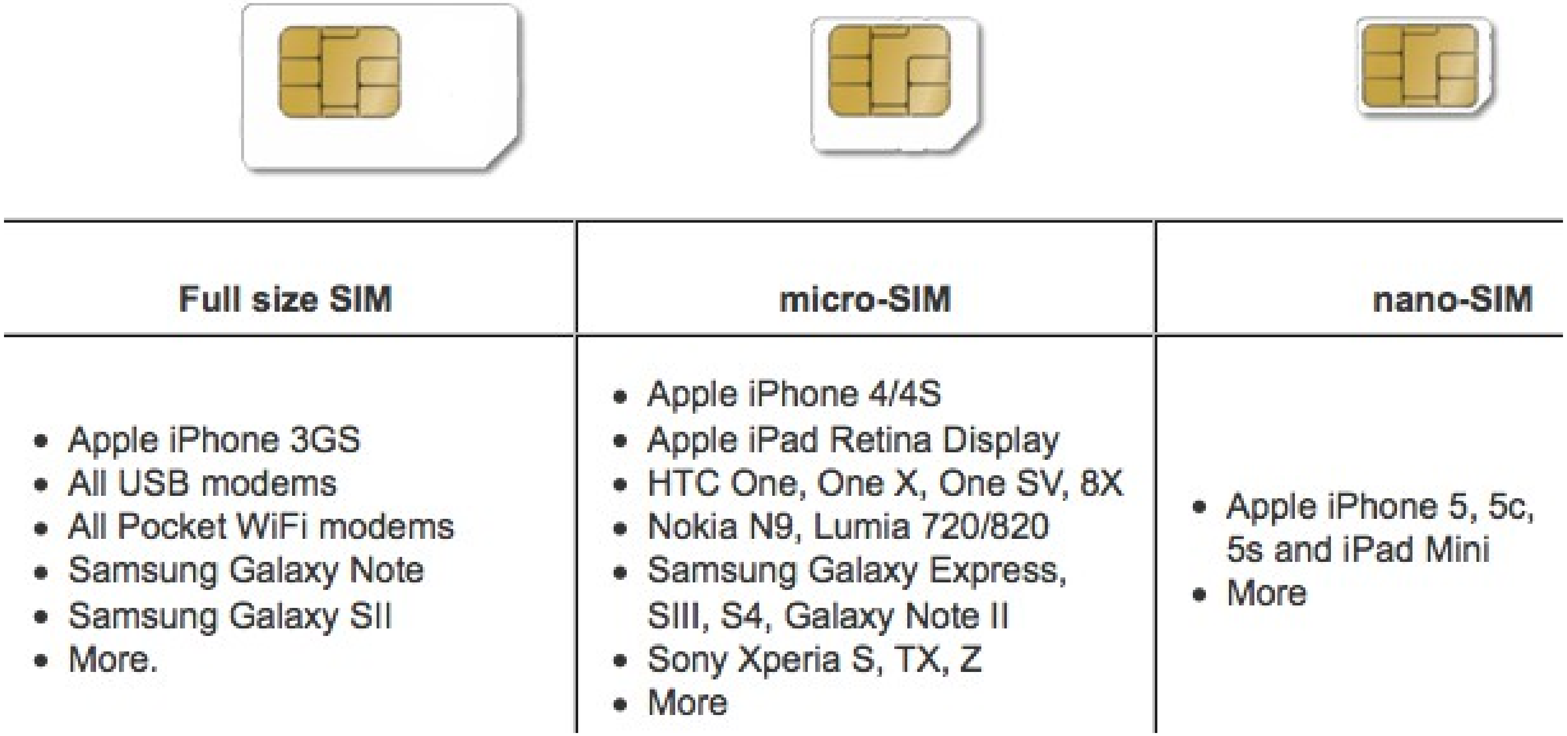


T-Mobile SIM Starter Kit - Nano SIM - No Annual Contract

Quantity: 1

Free!

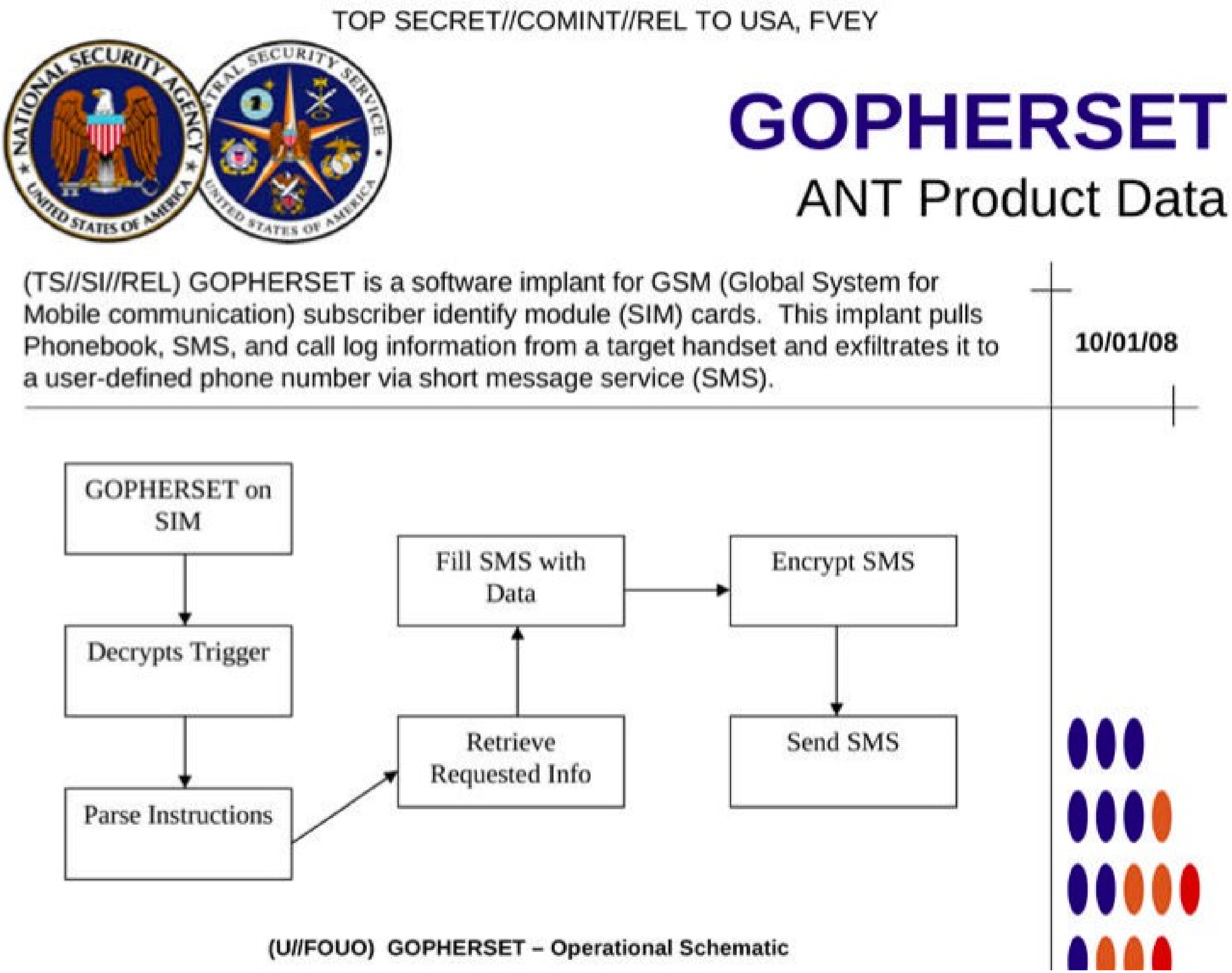
Change in size



Full size SIM	micro-SIM	nano-SIM
• Apple iPhone 3GS • All USB modems • All Pocket WiFi modems • Samsung Galaxy Note • Samsung Galaxy SII • More.	• Apple iPhone 4/4S • Apple iPad Retina Display • HTC One, One X, One SV, 8X • Nokia N9, Lumia 720/820 • Samsung Galaxy Express, SIII, S4, Galaxy Note II • Sony Xperia S, TX, Z • More	• Apple iPhone 5, 5c, 5s and iPad Mini • More

Source: Vodafone

Why to talk about SIM Security?



TOP SECRET//COMINT//REL TO USA, FVEY

GOPHERSET

ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

GOPHERSET on SIM

Decrypts Trigger

Parse Instructions

Retrieve Requested Info

Fill SMS with Data

Encrypt SMS

Send SMS

(U//FOUO) GOPHERSET – Operational Schematic

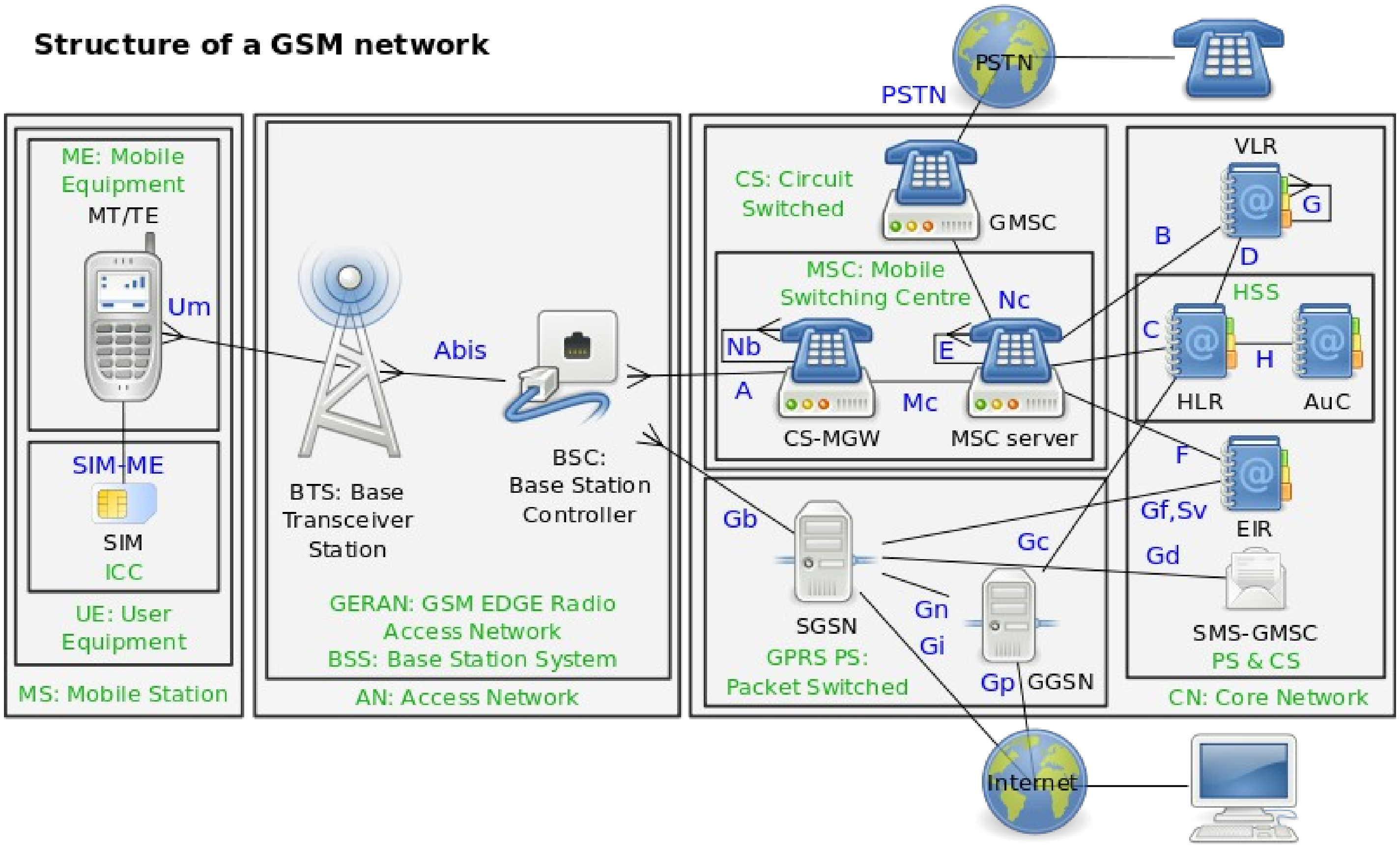
From Washington Post

Security in SIM cards

Features and functions

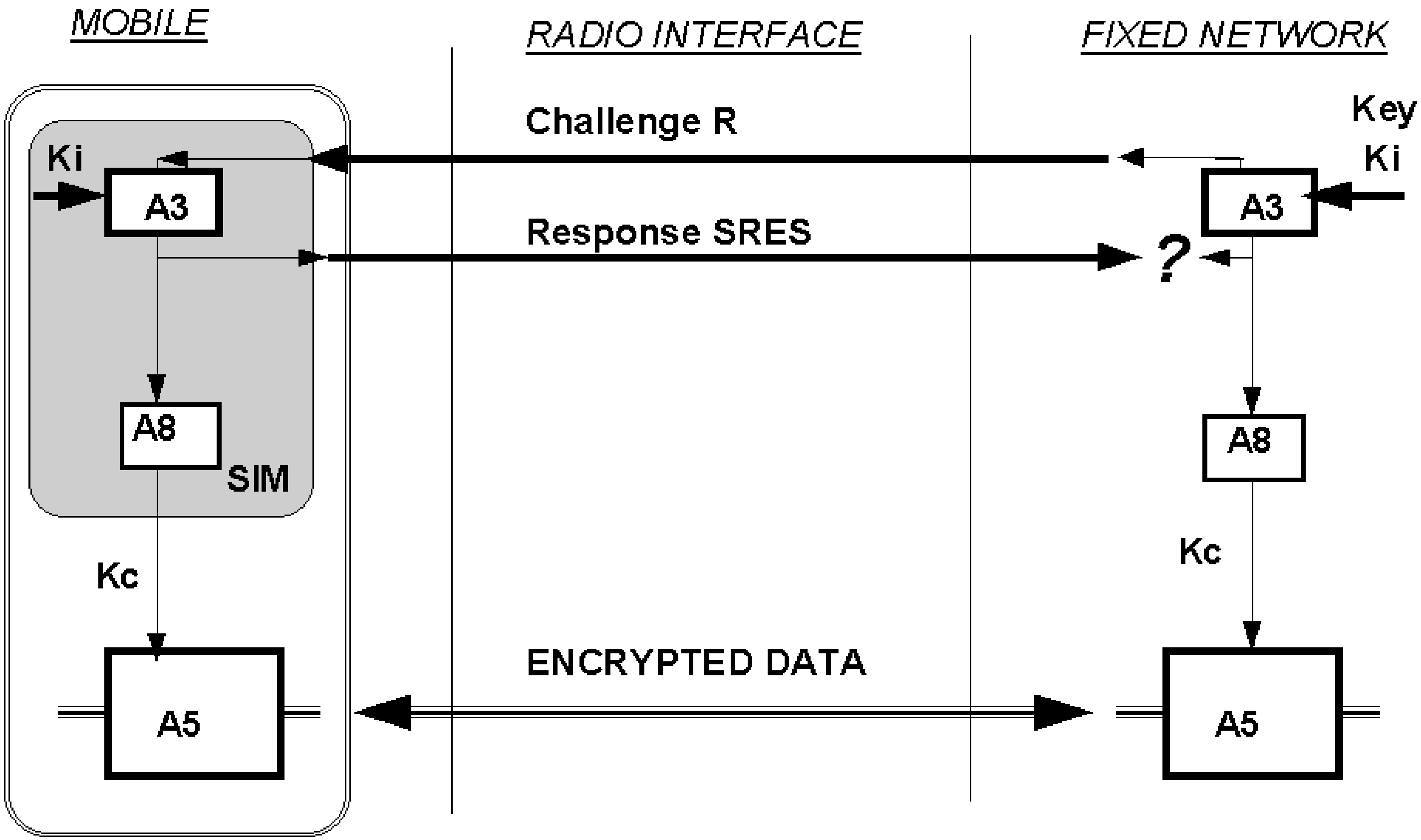
- **Identity and Access control** (IMSI, PIN code)
- **Authentication** to network operator (Ki, A3)
- **Confidentiality** (Kc, A8)
- Anonymity (TMSI)
- SIM application toolkit

GSM Background



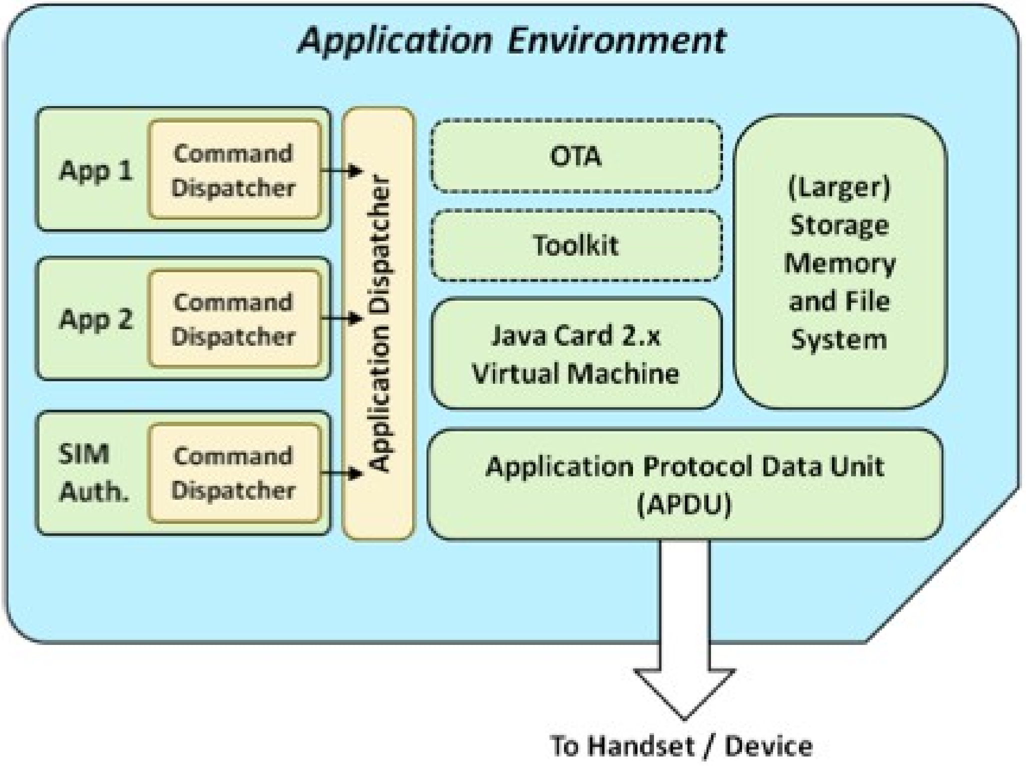
Thanks Kevin ;)

Authentication and Encryption



From 1994, Brookson

Current SIM architecture



Source: ofcom

Security attacks

- SIM Cloning (1998)
  - Comp128 leaked
  - Reverse engineered & cryptanalyzed

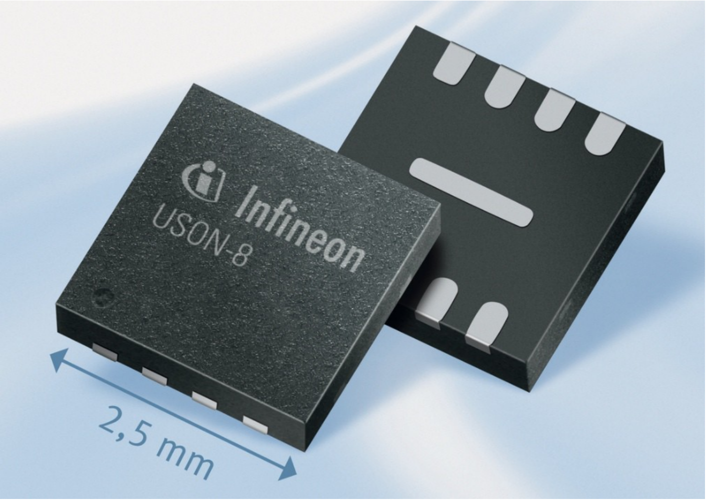
- SIM toolkit attacks
  - Fuzzing SMS
  - Send premium SMS
  - Mobile operators

- Cracking SIM Update keys
  - Recover DES OTA keys
  - Singed malicious applets with key
  - **https://wiki.thc.org/gsm/simtoolkit**

Changing Telco world

- Goal achieved in lat 25 years - " billions users connecting every continent "
- Next goal- "Connecting billions of devices (m2m devices, vehicles, IoT devices)"
- SIM to USIM to eSIM
- Embedded SIM vs Soft SIM
- New security architecture

Embedded SIM



- Designed for M2M devices
- Non-removable
- No Soft/virtual SIM
- New security standard
- No change in authentication / encryption to the operator
- Security architecture for remote provisioning

eSIM Standard requirements

- Contain one or more profiles
- **But ONLY one profile activeat a time**
- Behavior is same as in SIM or USIM
- Certification mandatory
- Satisfies “3G Security, Security Threats and Requirements” (TS 21.133)

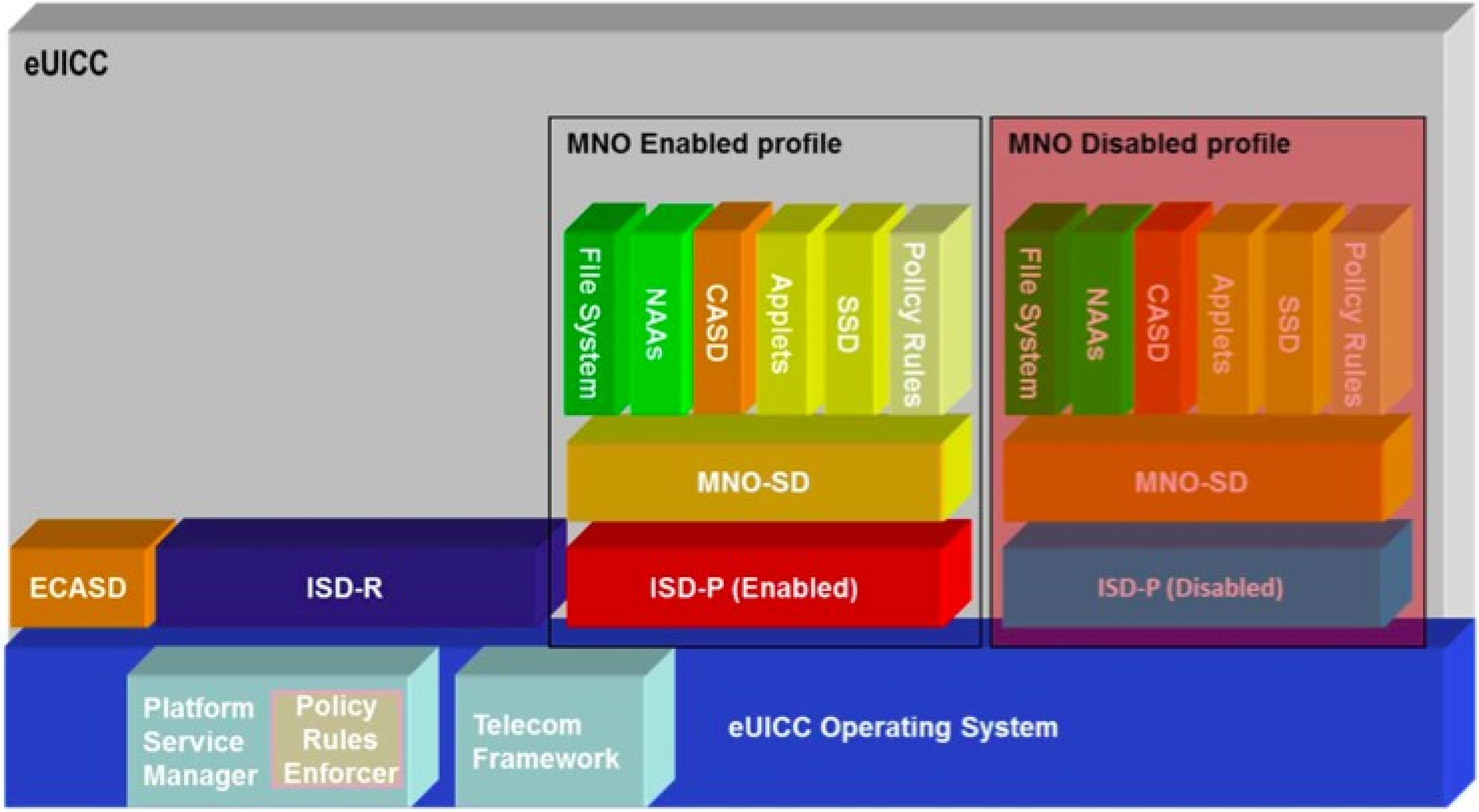
Remote Provisioning

- Challenge was to securely and **remotely** change Ki (Subscription)
- New card platform to support multi-profiles
- Introduced new network elements (SM-SR/SM-DP)
- Done over SMS or HTTPS connection
- Over-the-air packets encrypted with OTA keys

SM-SR : Subscription Manager – Secure Routing

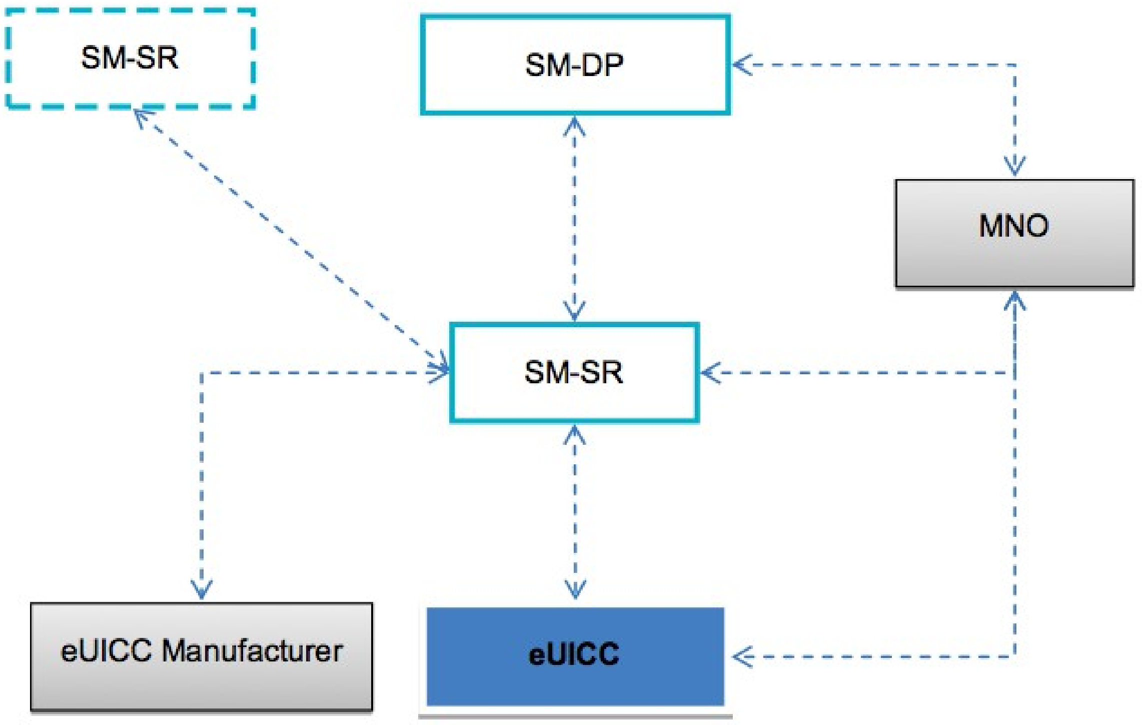
SM-DP : Subscription Manager – Data Preparation

Card Architecture



Source: GSMA

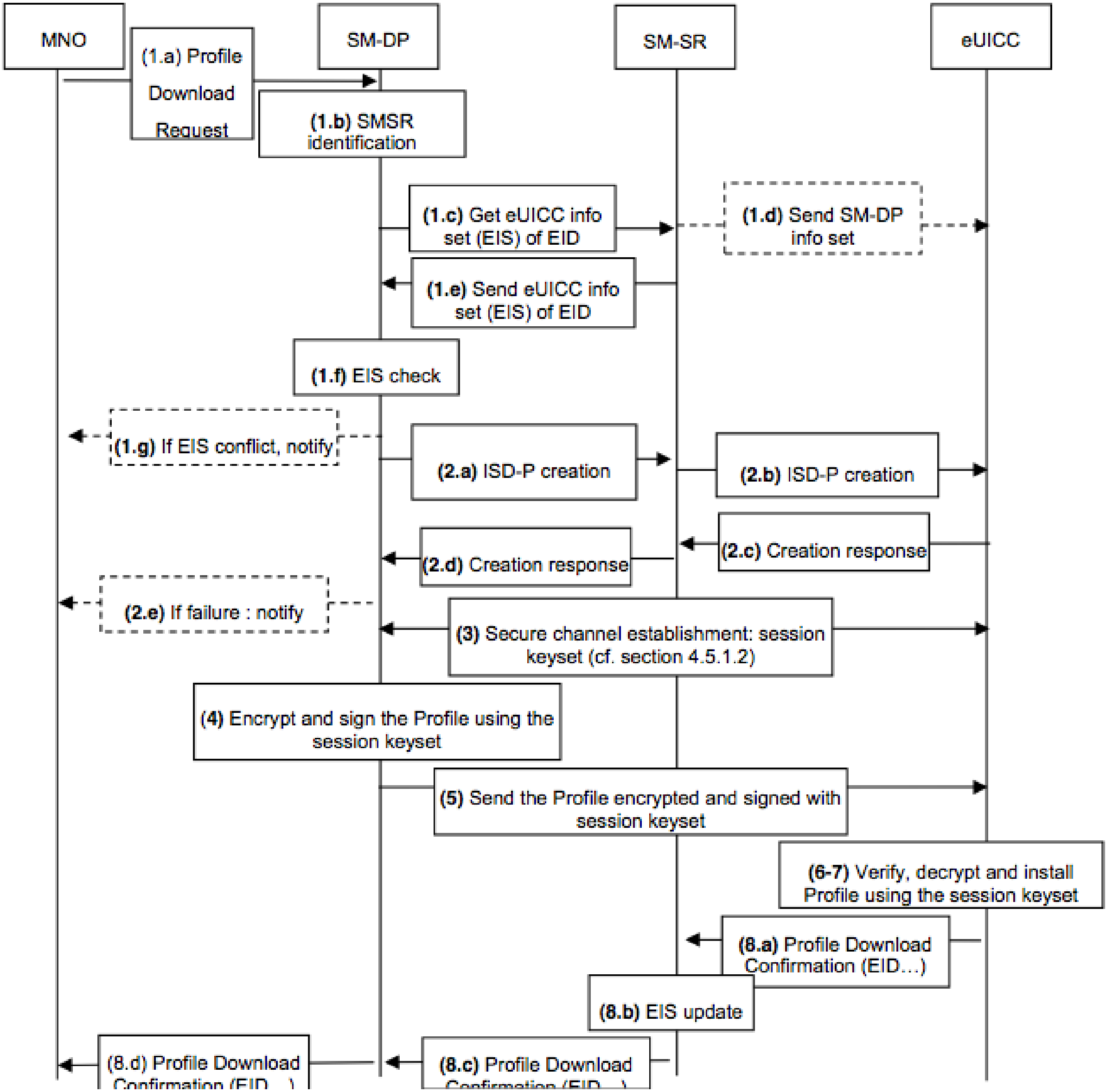
Remote provisioning architecture



Source: GSMA

Ref: 12FAST.13 - Embedded SIM Remote Provisioning Architecture

Example - change operator



MNO

SM-DP

SM-SR

eUICC

(1.a) Profile Download Request

(1.b) SMSR identification

(1.c) Get eUICC info set (EIS) of EID

(1.d) Send SM-DP info set

(1.e) Send eUICC info set (EIS) of EID

(1.f) EIS check

(1.g) If EIS conflict, notify

(2.a) ISD-P creation

(2.b) ISD-P creation

(2.c) Creation response

(2.d) Creation response

(2.e) If failure : notify

(3) Secure channel establishment: session keyset (cf. section 4.5.1.2)

(4) Encrypt and sign the Profile using the session keyset

(5) Send the Profile encrypted and signed with session keyset

(6-7) Verify, decrypt and install Profile using the session keyset

(8.a) Profile Download Confirmation (EID…)

(8.b) EIS update

(8.c) Profile Download Confirmation (EID…)

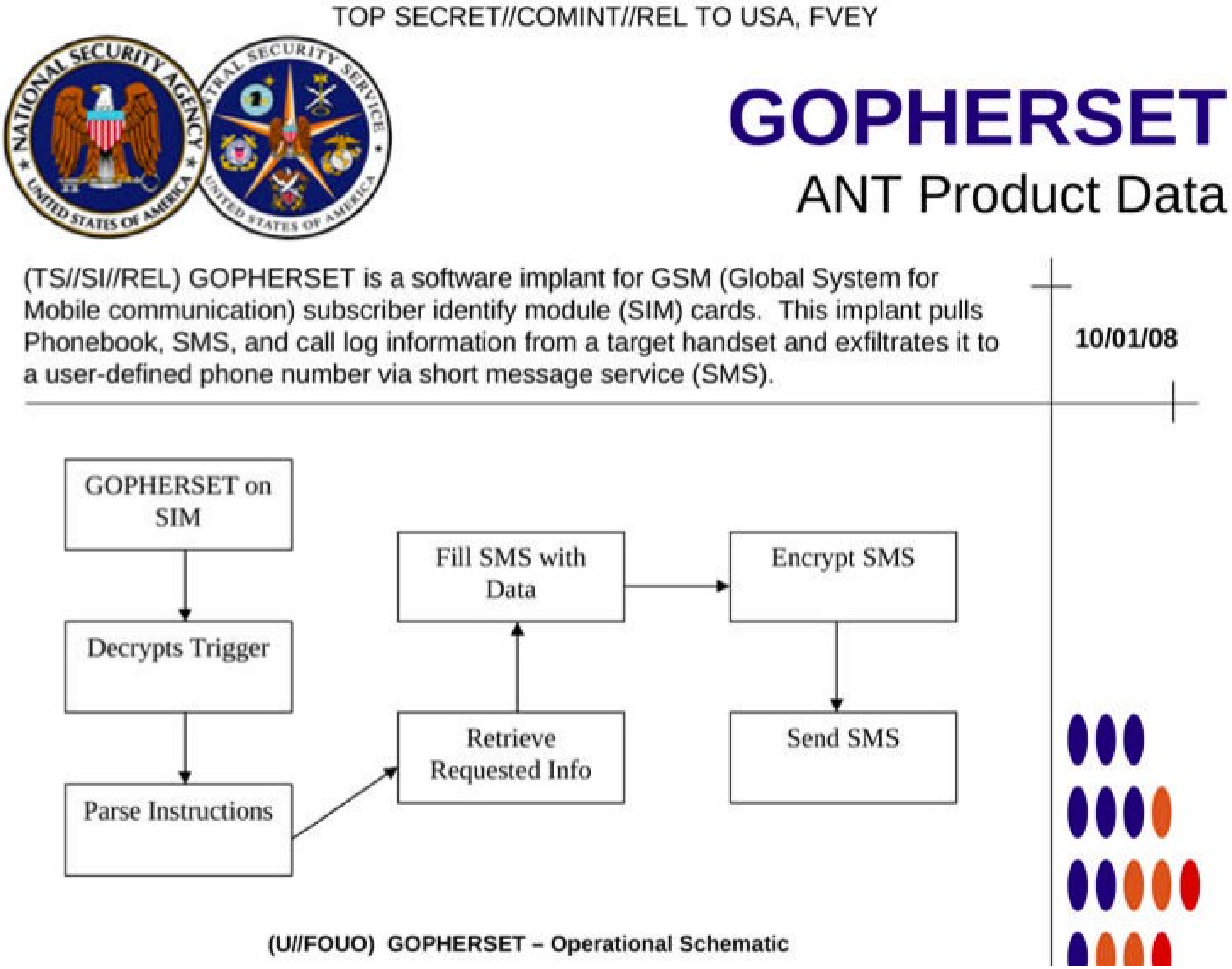
(8.d) Profile Download Confirmation (EID…)

Source: GSMA

Security threats

- Over-the-air attacks (DoS)
- Hardware attacks
- Privacy Issues (who owns what?)
- eSIM (cloning? Jailbreak?)
- Device theft?

Implant for eSIM??



TOP SECRET//COMINT//REL TO USA, FVEY

GOPHERSET

ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

GOPHERSET on SIM

Decrypts Trigger

Parse Instructions

Retrieve Requested Info

Fill SMS with Data

Encrypt SMS

Send SMS

(U//FOUO) GOPHERSET – Operational Schematic

From Washington Post

Thank you!