**3GPP TSG SA WG3 Security — S3#10** **S3-000052**

**19-21 January, 2000**

**Antwerpen, Belgium**

**Source: BOSCH**

**Title:** : "**3GPP terminal identity security: levels, requirements and mechanisms"**

**Document for:** Discussion /decision

**Agenda Item:** Terminal security 8.3

**This is a living document to discuss the present and future security levels of terminal identity (IMEI). The requirements and services are defined for each security level in consideration. Possible basic mechanisms are proposed to evaluate the impact of secure identity on 3GPP Security Architecture.**

**The first version of this document is prepared based on Doc s3 99-401 based on [1] to [10] which includes a digest of S3 documents presented so far. Doc s3 99-439 is also involved, it includes a proposal for essential requirements for secured terminal identity for 3GPP terminals.**

Two security levels are identified, protected IMEI without provability and protected IMEI with provability.

## 1. Protected IMEI without provability (current GSM status)

### 1.1 Requirements:

The requirements are defined after being improved by change request [4] (CR to GSM 02.09 V4.4.0, Doc AP99-093). The wording is as follows:

1. ***It shall not be possible to change the IMEI after the ME's final production process. It shall resist tampering by any means (e.g. physical, electrical or software)***

2. ***The security policy for the Software Version Number (SVN) is such that it cannot be readily changed by the user, but can be updated with changes to the software.***
   ***The security of the SVN shall be separate from that of the IMEI.***

Fig.1 shows a basic discussion scenario to realise these requirements.

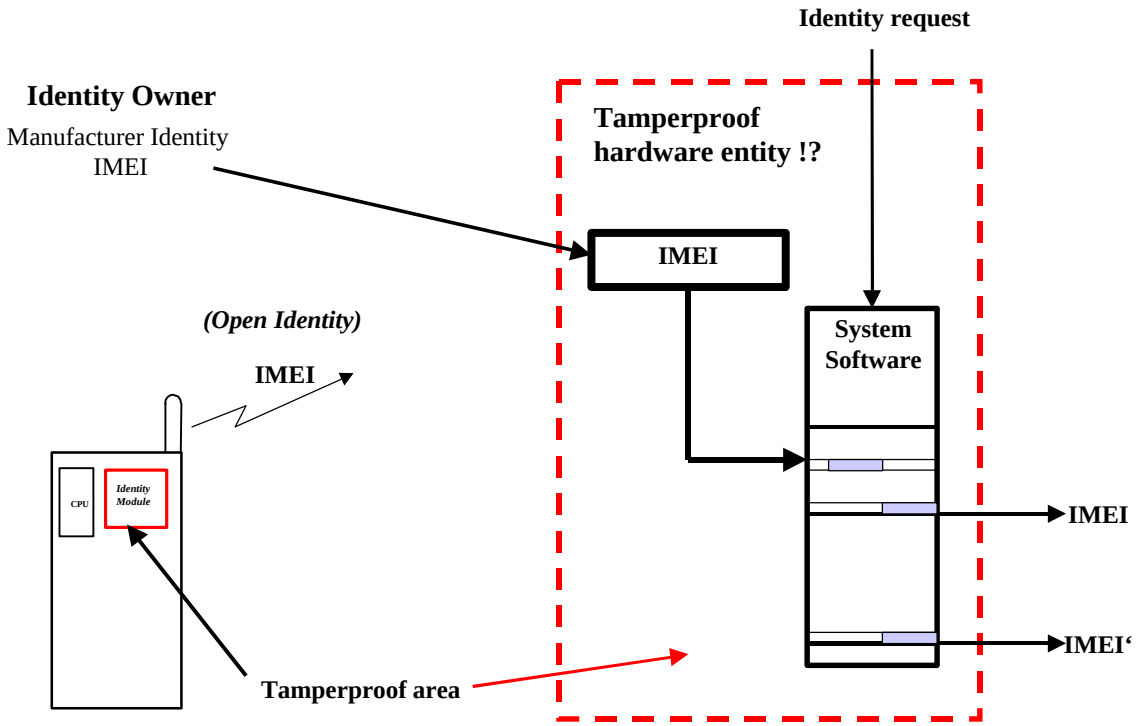


**Fig. 1 Current Terminal Identity concept in GSM**

## 1.2 Security level

IMEI is sent in clear (open identity). The following characterise the security of that terminal identity

- No proof of origin or type approval is possible
- Cloning is basically possible. As sending an arbitrary IMEI is always possible from other terminal or other software source.
- A certain terminal can not be securely identified if the software is not provable.
- If the software is secured then IMEI is secure (software dependability). No secured software execution is known without cryptographic means.
- Network failed in GSM to control illegal terminals whatever the reason is for such control.

It is noted that the software security can not be separated from IMEI security and vice versa. The reasons are:

- The software is the last source of IMEI ( the entity which physically delivers IMEI). The stored IMEI is not necessary the same as the sent one
- If the software can be changed, then any forged IMEI could be sent. Many attack scenarios are possible
- If the software is made provable, then IMEI could be seen as somehow secure. However a substitution attack is always possible (one scenario is to substitute the software with other copied piece of software which delivers a forged IMEI).

- A basic security rule is violated in this system. “unidentified entity is a part of the system”, this eases substitution attacks. The same holds for the base station.

**As a result of this discussion the above mentioned requirement No. 2 appear to be contradictory !!**

### 1.3 Usage/relevant service:

- Deter using stolen terminals
- Blacklisting type non-approved terminals
- Identify emergency call terminal
- SIM lock

### 1.4 Impact on security architecture:

No impact. The methodology to protect IMEI by manufacturers is up to the manufacturer, as no common proof mechanism is necessary.

### 1.5 Advantages:

1. Relatively simple to realize
2. No standardization is necessary

## 2. Protected and provable IMEI

A cryptographically secured IMEI is proposed for 3GPP to cope with future 3GPP requirements and applications

### 2.1 Requirements proposal (source Bosch Telecom):

1- An open IMEI and its corresponding secret part SIMEI is to be stored in a non-volatile memory in a tamperproof physical entity which is hard to remove from the terminal
2- A common proof algorithm is to be defined to cryptographically prove that the SIMEI corresponding to IMEI resides in the terminal.
3- IMEI should not be easy to modify, but if modified the proof algorithm should fail (see also 7)
4- The manufacturer should electronically sign IMEI before leaving the factory. No body other than the manufacturer should be able to generate equivalent signature.
5- Any operator and other legitimate party should be able to offer a time varying challenge to the terminal to prove the manufacturer signature. The manufacturer publishes some open or secret means to enable the proof of its signature (prove terminal origin and thus the originally manufactured terminal quality and capability).

6- The terminal should include multiple provable mobile identities MI's as IMEI which could be separately defined by other identity owners as operator, user, regulator, authority and others (64 **MI**'s with 64 Bits and corresponding **SMI**'s with 128 Bits each appear to be adequate for future needs). The same scenario 1 to 5 should be possible.
7- The signature SIG should also be possible to be generated from many predefined SMI's and many predefined challenges CH's.

8- It should be possible to modify MI and SMI by the owner of SMI by presenting SMI again to the tamperproof device. This is to enable the reuse of identities by legal identity owners.

### 2.2 Security level

IMEI is sent in clear together with its (time variant challenged) proof of signature . The following characterise the security of that terminal identity

1- Proof of origin or type approval is possible

2- Cloning is not possible. As imitating the right signature needs the secret SIMEI.

3- A certain terminal can be securely identified either if the software is not secure. No dependency between software and identity.

4- Network can identify and control illegal terminals to carry out any relevant security action without destroying other services.

### 2.3 Usage/relevant service:

- Deter using stolen terminals
- Blacklisting type non-approved terminals
- Identify emergency call terminal

- Restricting some service to some class of terminals with special quality
- Effective implementation of the MExE and Mobile IP security requirements
- Secured SIM lock

## 2.4 Impact on security architecture:

As standardised architectures are necessary, the following possible impact on security architecture is identified.

### 2.4.1 Architecture/possible mechanisms (source Bosch Telecom):

A common methodology to proof IMEI via common proof-mechanism is necessary.

If a provable identity is to be integrated and standardized in the 3GPP terminals, the following two technical requirements appear to be essential:

### 2.4.2 Hardware Requirements

To be able to cryptologically identify a unique terminal, the following two physical entities are essential: (Fig. 2 shows one concept for a basic IMEI security infrastructure)

1. A tamperproof **write-only** secret nonvolatile identity to store **SMI (1..64) with 128 Bits each** (whatever *tamperproof* means in the current state of the art technology). The corresponding **MI (1..64)** with 64 bits each is also stored not necessarily protected in a write once /read non-volatile memory

2. Define a *commonly known* Signature Function **SF**. This could be achieved by using:

   ***Either*** **(SF1):** a one way function ( say f8 or f9 or as in [6]) which maps this secret identity SMI or many identities SMI1, SMI2....and a challenge CH or many challenges CH1, CH2....into a signature response SIG to prove the existence of the secret identities in the terminal

   **SIG = SF1 ( /SMI1,SMI2../ , /CH1, CH2.../) (symmetric function)**

   ***Or (SF2)*** **:** some public-key one way function SF2 (say squaring function as Rabin-Lock) [7] which proves the existence of the write-only secret identities in the terminal.

   **SIG = SF2 (/SMI1, SMI2..../, /CH1, CH2 .../) (asymmetric function)**

   There should be no hardware possibility (trap door) to read any SMI.

   The tamperproof device should be physically tied into some terminal core function.

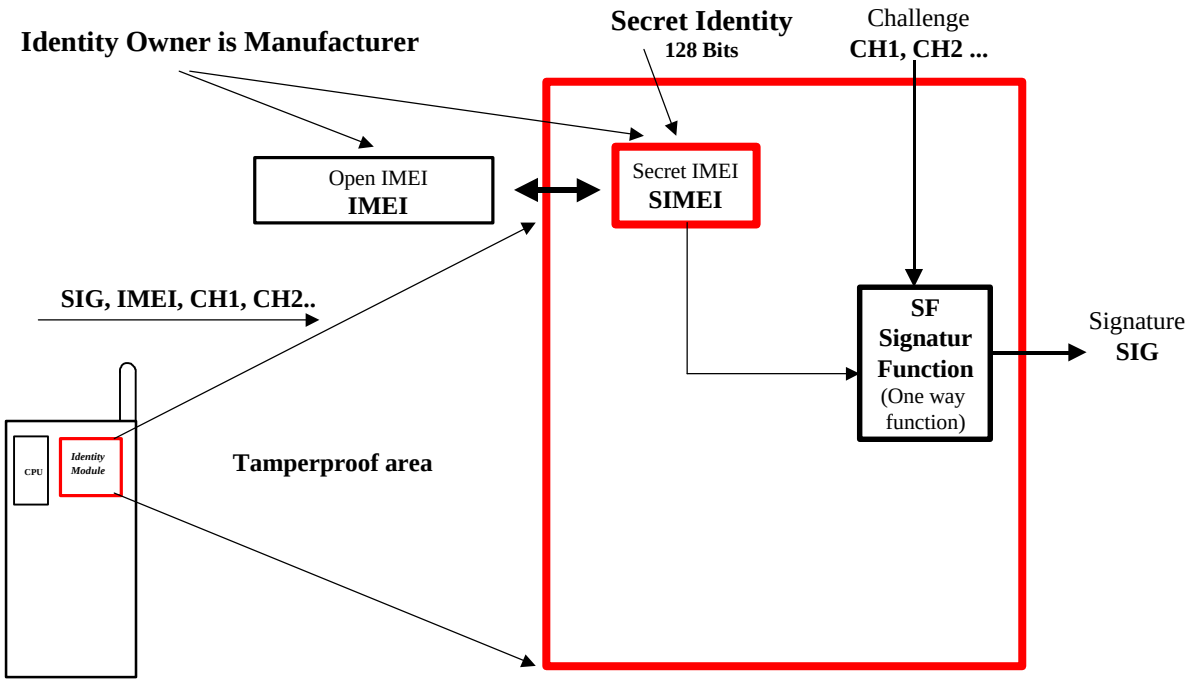


**Fig. 2 Basic IMEI security infrastructure for 3GPP**

Fig 2 shows a basic possible IMEI security infrastructure for 3GPP.

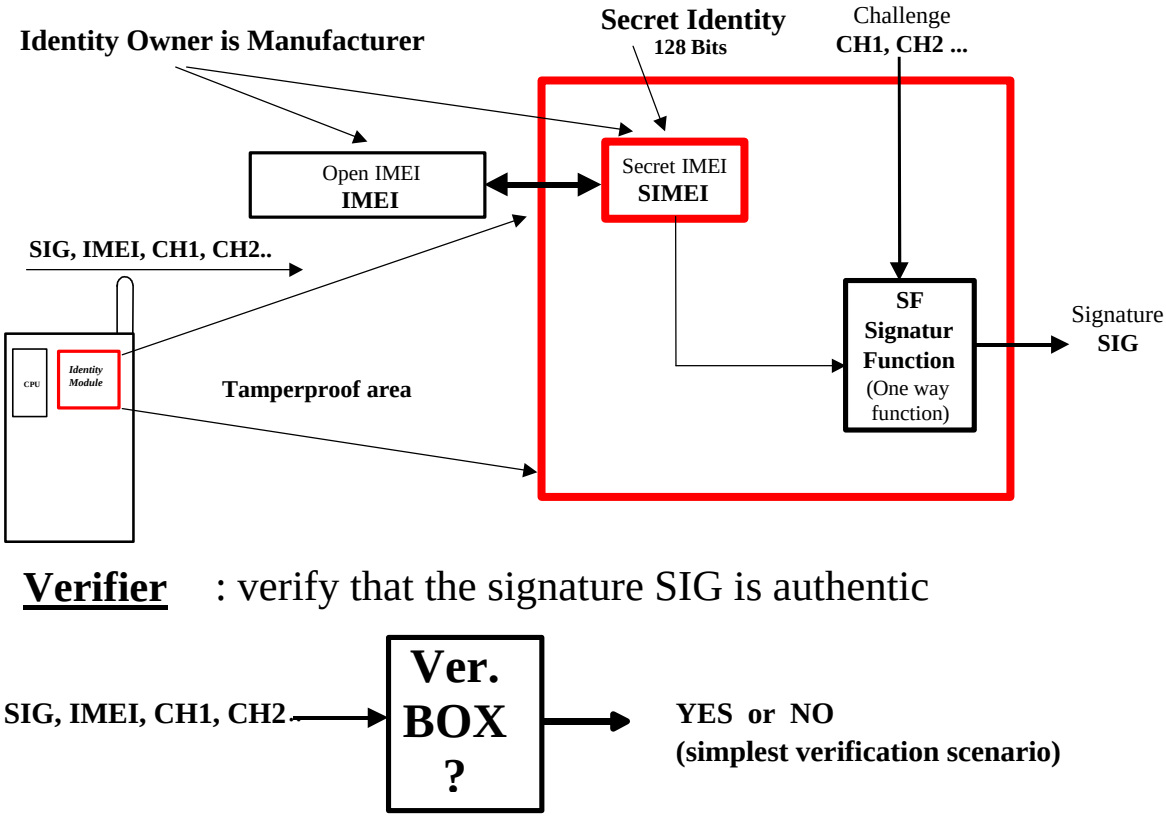


**Fig. 3 Simple verification scenario**

**Example scenario:**

Fig 3 shows a possible simple scenario to check the IMEI put into the terminal by the manufacturer. The verifier should be able to challenge the terminal and get as response the vector:

**(SIG, IMEI, CH1, CH2, )**

Where:

**SIG:** the terminal response signature which includes a provable signature of the manufacturer

**IMEI :** is the open terminal identity used in GSM (serial no. with manufacturer identification)

**CH1, CH2:** time variant random challenges from terminal and verifier

This scenario **proves** that

- **IMEI is correct**
- Terminal is **signed by the manufacturer** and had after being manufactured the specifications defined by the manufacturer

The scenario counteracts terminal theft and cloning . The signature proves also that the terminal had at the time of manufacturing some technical qualifications.

The verification box **Ver. BOX** in Fig. 3 :

- should not include a large data base
- should not need frequent updates to verify manufacturer signature

- should not maintain large IMEI lists.
- .....

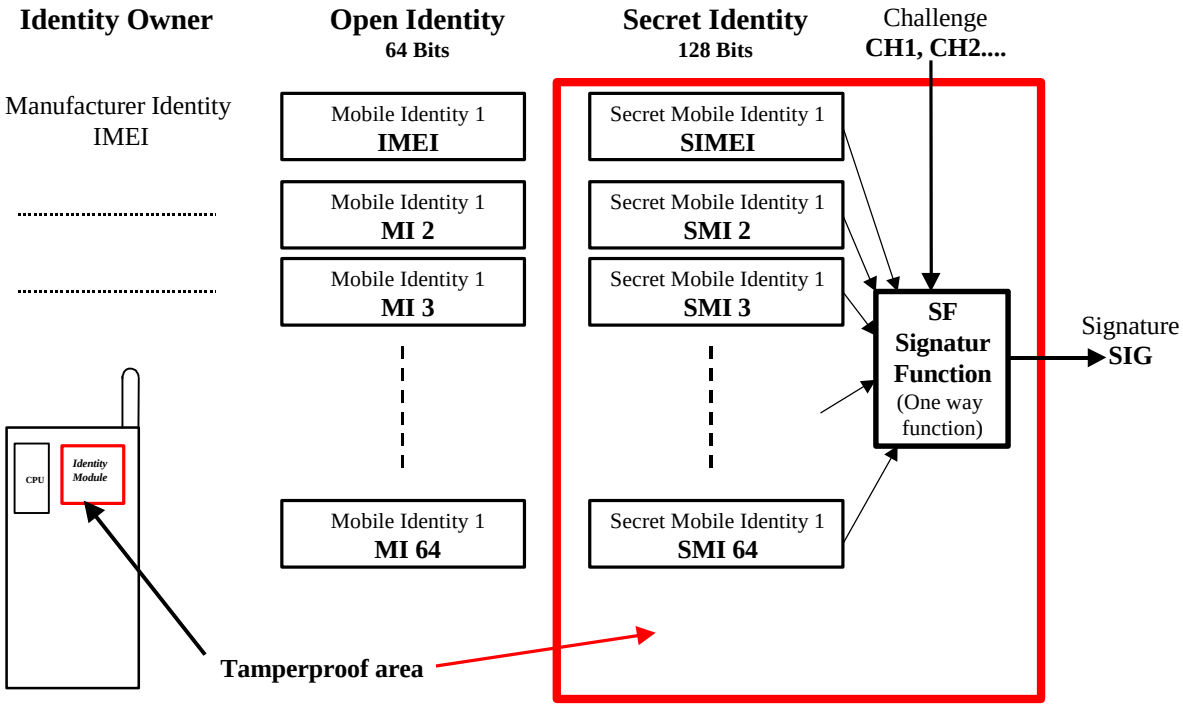


**Fig. 4 Proposed secured identity infrastructure for 3GPP terminals**

Fig 4 shows a proposed muti-profile secured identity infrastructure to be as a common standard in future 3GPP terminals.

### 2.4.3 System Requirements

These requirements are highly application and protocol dependent (tbd).

1. One or many **system protocols** which proves the identity for relevant applications
2. A **central data base** for some applications. This should be avoided as far as possible

## 2.5 Advantages:

3. Relatively simple to realize (probably without maintaining large and distributed data bases)!
4. Cloning and theft could be prohibited
5. Secured proof of origin and terminal type/class are supported
6. Identification security does not depend on software security
7. Identification function do not disturb other system functions. It could be made optional
8. New application horizons in 3GPP !

**References:**


[1] Charles Brookson, DTI,UK, Terminal Security: Requirements for a Secure Identity
A draft discussion document, included in Doc. s3 99-401.

[2] Security mechanisms for the IMEI, Ericsson, s3-99 296

[3] Provable Terminal Identity , Status and future applications, Bosch . Doc s3-99250.

[4] CR to GSM 02.09 V4.4.0, Doc AP99-093

[5] Change Request to GSM 02.09, GSM 02.16, GSM 03.03 and GSM 11.10 to ensure IMEI security . Doc s3-99214.

[6] Secret-Key Mechanisms for Secured Terminal Identification , Bosch, Doc s3-99127.

[7] Provable Terminal Identity with a Public-Key Mechanism, Bosch, Doc s3 -99168

[8] The use of Zero-Knowledge Identification mechanisms for 3G Terminal
Identification , Vodafone, Doc s3-99303.

[9] Repor 3GPP TSG-SA WG3 (Security) t to SA Meeting # 4,Miami, 21-23 June 1999 Michael Walker Chairman 3GPP TSG-SA WG3 Doc s3-99293

[10] Proposal for IMEI Security, Mannesmann, T-Mobil, Doc s3-99106.

[11] Mobile Station Application Excution Environment (MExE) 3G TS 23.057 V1.3.0