3GPP Terminal Identity Security

IMEI Security

Antwerpen 2000.01.20

Wael Adi

Meeting #10, DOC. S3-000071

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

1. Protected IMEI without provability (current GSM status GSM 02.09 V 4.4.0)

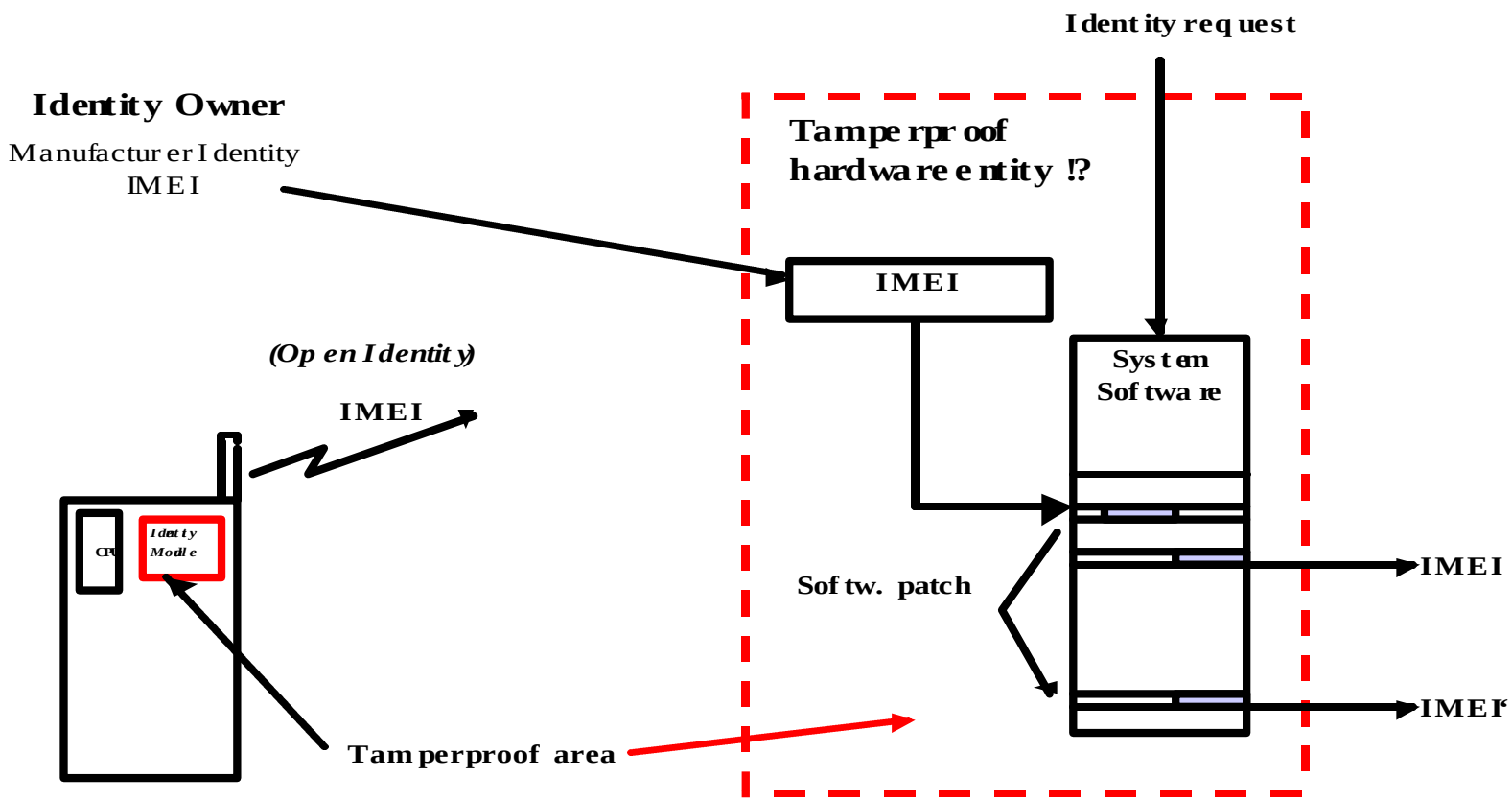
Requirements:

(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.

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.



© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

Security weaknesses

- IMEI is sent in clear (open identity)
- No proof of origin or type approval is possible
- Cloning is basically possible
- IMEI function in GSM failed till now
- IMEI security depends on software security

As a result, requirement No. 2 appears to be contradictory !!

Basic security rule is violated:
”un-identified entity is a part of the system”

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

Usage/relevant service:

-Deter using stolen terminals

-Blacklisting type non-approved terminals

-Identify emergency call terminal

- reliable SIM lock ...

- ***All these applications are unreliable/failed in GSM !***

Impact on security architecture:

No impact. Methodology is up to the manufacturer

Advantages:

.Relatively simple to realize

.No standardization is necessary

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

2. Protected and provable IMEI (proposal basics)

Requirements (source BOSCH):

- An open **IMEI** and a corresponding secret part **SIMEI** is to be stored in a non-volatile memory in a tamperproof physical entity which is hard to remove, replace, read...
- A **common proof algorithm** is to be defined (for global identification)
- IMEI should not be easy to modify. If modified, then it should always be detected
- The manufacturer should electronically sign IMEI
- A third party should be able to verify the manufacturer's signature
- The terminal should include 64 such independent identities with 128 bits/each for separate use by owners, operator, user, authority etc.
- It should be possible to modify Identity if the secret part is presented.

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and posing on to third parties.

Protected and provable IMEI

Security level

IMEI is cryptographically signed (proof of signature)

-Proof of origin or type approval is possible

- Cloning is not possible.

- Terminal securely identified either if the software is not secure

-Network can identify terminals without destroying other services

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

Protected and provable IMEI

Usage/relevant service:

- Deter using stolen terminals
- Blacklisting type non-approved terminals
-Identify emergency call terminal
-Restricting service to some class of terminals with special quality
-Effective implementation of the MExE and Mobile IP security
-Secured SIM lock ... others

Impact on security architecture:

Standardised architectures are necessary

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

Impact on security architecture

1. A tamperproof **write-only** secret nonvolatile identity

   SMI (1..64) / 128 Bits each (whatever t*amperproof* is)

   MI (1..64) /64 bits each similarly stored (but readable)

2. Define a **commonly known** Signature Function **SF**.

Either ***(SF1):*** a one way function (say f8 or f9)

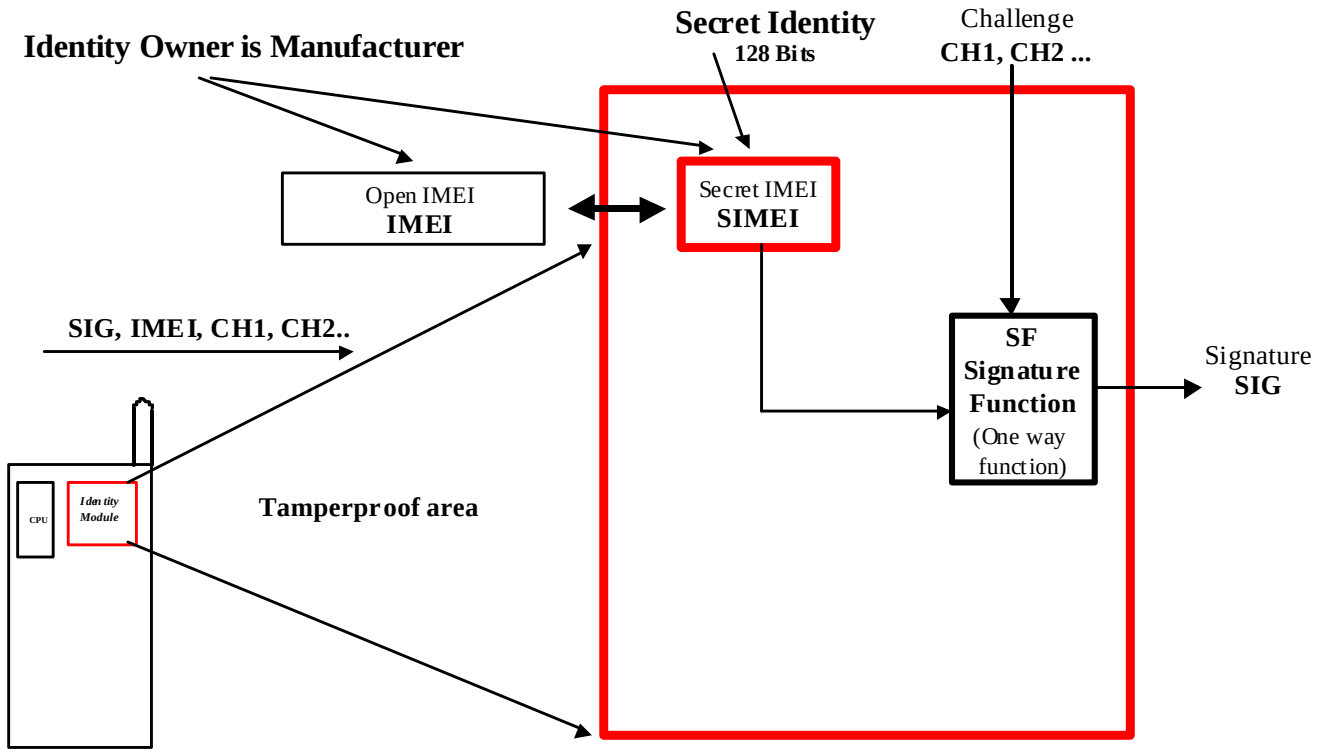
SIG = SF1 (/SMI1,SMI2../ , /CH1, CH2.../)

Or ***(SF2)*** **:** some public-key one way function (say Rabin-Lock)

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

- No (trap door) to read any SMI. SMI is physically tied to some core function.

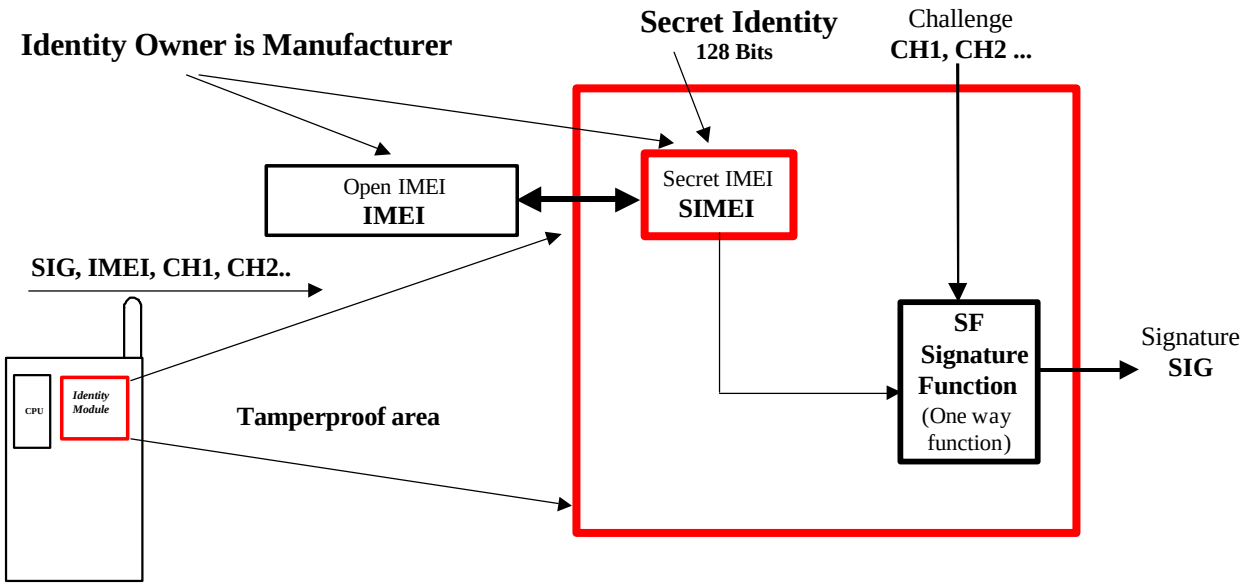
© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and posing on to third parties.



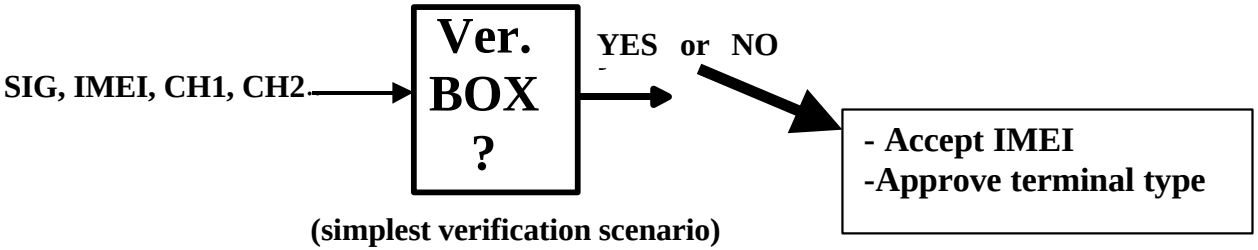
© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

BOSCH

Basic IMEI security infrastructure

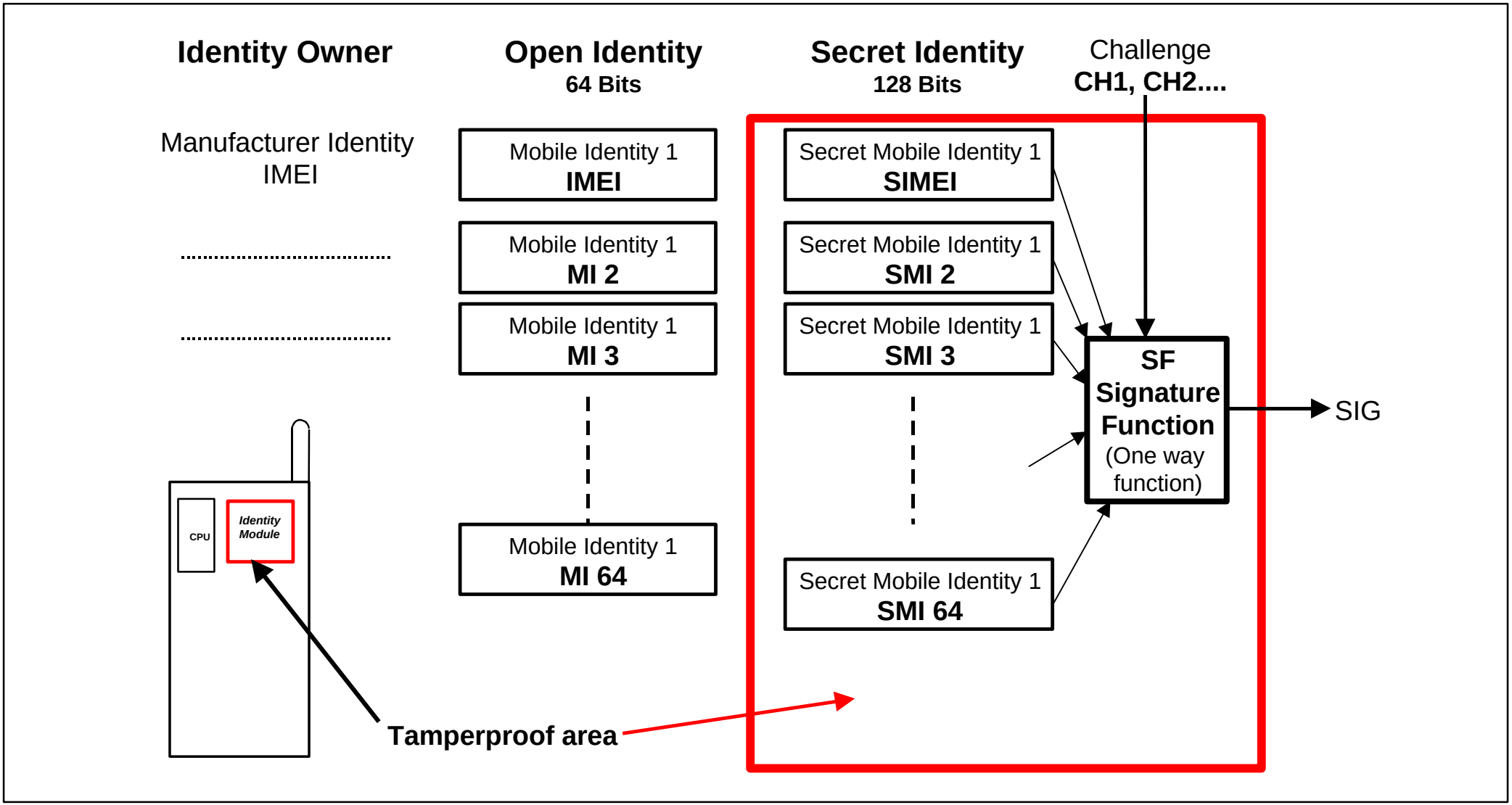


Verifier : verify that the signature SIG is authentic



(simplest verification scenario)

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.



© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

BOSCH

Secured Identity Infrastructure for 3GPP Terminals

Advantages of the proposed architecture:

- Relatively simple to realize (probably without data base)!
- Cloning and theft could be prohibited
- Secured proof of origin and terminal capability are supported

  (service restriction to certain class of terminal is possible)
- Identification security does not depend on software security
- Identification functions do not disturb other system functions

  (secured identification could be kept optional)
- New application horizons in 3GPP ... !

© Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.