GSM ASSOCIATION

EICTA

European Industry Association | Information Systems Communication Technologies Consumer Electronics

Security Principles

Related to

Handset Theft

Table of Contents

Change control – This document is under the shared revision control of GSMA, representing the operator community and EICTA representing the manufacturer community.

EICTA CCIG Doc Ref:	Eicta Doc: 04cc100
GSMA Doc Ref:	Security Principles Related to Handset Theft 3.0.0

Glossary of Terms

A shared EIR (SEIR) is effectively a piece of common EIR equipment run by or on behalf of a group of operators, most probably as a national grouping.

The Central EIR (CEIR), hosted by GSMA, maintains information on the eligibility for access to networks by Mobile Equipment Types. The CEIR interconnects with Equipment Identity Registers (EIR) through out the world so that a common set of data is maintained and available to participating operators.

Other commonly used terms are defined in the ETSI standard GSM 01.04 version 8.0.0 Release 1999 which is available to download at;

http://www.3gpp.org/ftp/Specs/html-info/0104.htm

1. Introduction

The IMEI was originally introduced, as a unique terminal identity, for type approval reasons, in order that non-type approved terminals could be prevented from connecting to GSM networks. Nowadays, the IMEI is used to identify mobile station equipment on mobile networks in order to be able to take measures against the use of stolen equipment or equipment whose use can not be tolerated under Article 7 of the R&TTE directive (within Europe), or an appropriate regulatory requirement in other markets. Additionally, the IMEI can be used to allow infrastructure to load appropriate patches and adaptations to avoid inter-working issues.

All reasonable efforts should be made to protect the integrity of the IMEI value and the write access to the value should only be available by a mechanism determined by the manufacturer. Despite the need for GSM terminals to have unique identities, in practice IMEIs have been tampered with. The GSM specifications (e.g. ETSI/3GPP spec 122.016) were changed in Nov 1999 to provide that;

> *"The IMEI is incorporated in an MS module which is contained within the MS equipment. The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).*
>
> *NOTE: This requirement is valid for new GSM MEs type approved after 1st June 2002. However, this requirement is applicable to all UEs of UMTS from start of production.*
>
> *This implementation of each individual module should be carried out by the manufacturer who is also responsible for ascertaining that each IMEI is unique and keeping detailed records of produced and delivered MS."*

Evidence provided by GSM operators indicates that, while most handset manufacturers have made progress to protect the IMEI, improvement is required by the manufacturing community as a whole.

1.1 Importance of IMEI Integrity

Handset theft has emerged as a serious and growing cause for concern in the cellular industry and the GSM Association's Board has indicated its commitment to tackle the issue head on. The GSM Association is undertaking a concerted drive to extend the use of Equipment Identity Registers (CEIR & EIR) across the global GSM operator community to ensure stolen handsets can be barred from networks by using the handsets' IMEI numbers.

While the EIR was originally specified as a tool to bar network access to certain handsets its effectiveness is largely dependent on a secure implementation of the IMEI. Therefore, it should be realised that the use of CEIR/SEIR/EIRs does not represent the finite solution to handset theft and CEIR/SEIR/EIR deployment should be complemented by the efforts of the handset manufacturing community to ensure that all handsets delivered to market incorporate appropriate security features. The enhancement of IMEI integrity should be designed to ensure that EIRs/CEIRs/SEIRs work more effectively.

1.2 Improved IMEI Integrity Principles

Although GSM TS 122.016 clearly mandates that IMEIs should not be changeable after June 2002, the specification does not indicate any details on implementation characteristics. In order not to stifle innovation, the GSM Association and EICTA do not propose to mandate a standardised way to achieve IMEI integrity but it is desirous to set out handset security principles to provide guidance to handset manufacturers and to provide operators with a set of high level criteria against which handset security can be assessed.

1.3 Improved Regional Theft Guard Principles

Having studied the handset theft issue, EICTA-CCIG and the GSM Association believe that the aim of greatly reducing handset theft would be achieved more effectively if an additional mechanism were added to the solution. We believe this is necessary to counter the export of stolen handsets outside of the EU.

If we assume that, in the future, many networks are connected to the CEIR and that IMEI integrity is improved so that IMEIs are proportionally resistant to change, there will still be a market in stolen handsets. The CEIR and secure IMEI only address the use of stolen handsets within those markets connected to the CEIR. Despite the best efforts of the GSM Association, it is not anticipated that all networks around the world will connect to the CEIR. Since handsets are commodity items there is an expectation that handsets stolen in territories connected to the CEIR will be shipped to networks not connected to the CEIR, maintaining a viable international trade in stolen handsets.

To address this, EICTA CCIG, the GSM Association, and its Members are considering ways that can bolster the security offered by the CEIR and the secure IMEI implementation. We would like to investigate a concept called 'Regional Theft Guard'. Regional Theft Guard would lock a handset so that it would only function with SIM cards from operators operating within a certain geographic area. It is anticipated that, generally, this geographic territory would correspond to a nation state. Consequently if the handset is stolen it will not be possible to simply export it since it will refuse to accept SIM Cards from operators based in other territories. We believe that this is achievable using existing technology understood by the industry. It is intended to ensure that any solution proposed does not affect free circulation of handsets, the use a legitimate customer may make of their handset, or adversely influence competition.

Unfortunately, it has not been possible to complete investigations into the details of this proposal in the available time and, consequently, GSMA and EICTA will work on the Regional Theft Guard proposal and update the document once we have completed our investigations.

It is acknowledged that security is not absolute and the GSMA is not looking for guarantees that deployed security measures will never be broken. However, this document describes a number of high level measures that should be implemented to protect the IMEI,

2. Handset Security Principles

The following handset security principles are provided to help handset manufactures develop a comprehensive security architecture that facilitates the deployment of a range of solutions to protect the platform on which IMEI mechanism is stored.

2.1 Internal Resource Integrity

Principle 1 – Uploading, downloading and storage of executable code and sensitive data related to the IMEI implementation

Mechanisms should be implemented that are capable of;

- Validating the integrity of software resident on the platform e.g.
  - Detecting any alterations to data and/or software used for security purposes
  - Prohibiting operations designed to disable or bypass protection mechanisms
  - Maintaining trace logs of attempts to alter data and/or software

Manufacturers will consider how trace logs could be implemented without major impacts on memory or other resources.

Principle 2 – Protection of components' executable code and sensitive data related to the IMEI implementation

Mechanisms should be implemented to protect the executable code and sensitive data related to the IMEI implementation contents of various components against unauthorised modification. The data paths, from hardware data storage to emitted frames that include the IMEI to be presented to the radio interface, that handle sensitive data should be secured to ensure the IMEI value sent to the mobile network interface is unchanged and matches the IMEI value originally set by the handset manufacturer during the final production process, regardless of subscriber behaviour. The processing chain should be securely controlled and the control mechanism should be protected e.g. by using security buses.

Principle 3 – Protection against exchange of data/software between devices

In the absence of any relationship between hardware and software, data and software can be exchanged between handsets and this is one of the reasons why different handsets can contain the same IMEI. Therefore, the handset should incorporate a robust link between the handset hardware[1] and software to prevent cloning of components from one device to another. Data should be bound to the platform and protected from being exported to other handsets, possibly by using encryption keys or by linking the serial number of the micro-processor to the OTP ROM that contains the boot code.

It is accepted that, for logistical reasons, the software to be loaded to the terminal may be a 'vanilla' software that only gets secured to the terminal by the loading process (potentially by the terminal itself). This would allow terminals to have software upgraded in bulk using USB hubs etc. thus minimising the impact on the Manufacturer or Manufacturer Agent. It is not expected that each device will need to be programmed with an individual software that needs to be compiled on the 'programming PC' with the terminal's IMEI or similar.

[1] At least one electronic component containing memory and soldered on the PCB

2.2 Access Control and Partitioning for Handset Applications and Software

Principle 4 – Protection of executable code and sensitive data related to the IMEI implementation from external attacks

In order to mitigate the threat posed by malicious software, and to reduce the risk of reverse engineering, executable code and sensitive data related to the IMEI implementation should be inaccessible from outside of the handset.

In particular:

- Mere ciphering of secret information increases the risk of reverse engineering attacks as the handset needs the cipher value in clear form in order to check the secret information. The attacker then only needs to identify and extract the necessary ciphering elements and the ciphering method is then known for all handsets.
- All secret information pertaining to the IMEI implementation should be stored in hashed form to prevent observation and alteration if a software implementation is used and/or by using a hardened ciphering component in the case of a hardware implementation.
- There are various occasions on which data entered from outside the handset is validated by the handset. Mechanisms should be implemented in such a way that the information necessary to generate the data in the correct form is not accessible in software or readable hardware on the handset. An illustrative example includes:
  - If downloaded software is integrity protected with a symmetric algorithm, and the key for the algorithm is also stored in software on the handset, then this key allows the attacker to add valid integrity protection to other software.

Acceptable implementations could include measures such as:

- Storing one-way hashes of passwords (although these passwords need to be long enough to prevent exhaustive search)
- Integrity protecting software using public key algorithms, so that the verification key is different from the signing key.
- Implementing symmetric keys in unreadable hardware.

External access should be controlled in both read and write modes in a similar manner to how firewalls work. The handset could include a security controller (i.e. a trusted security kernel) which analyses the legitimacy of incoming queries. It should not be possible to have read access to "security parameters" from any extension port of the handset and no direct read access to the contents of the various internal resources should be permitted.

Domains could be implemented to facilitate the creation of a dedicated service applications zone which is reserved for the subscriber's use with domain separation protecting sensitive data of one process from being attacked by another process. Strong access control mechanisms should be implemented to ensure that only authorised access to internal resources is permitted.[2]

[2] The implementation of this principle should not adversely affect the handset download function (subject to the terminal's security policy) of Java middlets or applets.

Principle 5 – Prevention of download of a previous software version

The ability to download previous software versions could allow malicious attackers to circumvent implemented fixes and rollback to a previous software version should be prohibited, over the air or by rollback on the platform. A PKI solution could be deployed to ensure superseded software versions cannot be re-enabled.

It is accepted that there may be logistical reasons why a rollback to a previous software version is desired; for example if the latest software version introduced a (non-security related) flaw and the previous software version had no major flaws. Options for implementation are to be identified and are at the discretion of the manufacturers.

For illustration purposes only, if EQ.21 was an acceptable software version and EQ.22 was released to take account of changes to network operator names. If a name was spelled incorrectly in EQ.22, such as “Vodaphone UK”, and an Operator had 10,000 terminals in their stores and needed to get them to market, the quickest resolution would be to roll the software back to EQ.21.

We would request that this not be done and that a new software version, EQ.23, is compiled and released. It is acceptable that EQ.21 and EQ.23 are identical.

Principle 6 – Detection of, and response to, unauthorised tampering

To discourage unauthorised internal interference with the handset it may be desirable to render the handset useless as soon as an attempt to change the IMEI is detected by the handset.

2.3 Software Quality

Trusted software should not exhibit the vulnerabilities outlined in measures 7 and 8 and should be developed in accordance with well defined and rigorous software quality processes. Such processes should consist of enhanced documentation, analysis and design review prior to coding. Adherence to a trusted software development process should ensure the development of code that runs predictably and without security vulnerabilities.

Principle 7 – Software quality measures

A number of software quality measures should be applied for all sensitive functions. Although the list is not exhaustive, previously seen attacks suggest that some of the measures recommended, although not specifically requested to be implemented, include:

- A single input and output point for each function
- Stacked data should be erased before and after each function processing
- All incoming requests/input should be syntactically controlled before processing
- A single default processing value should be defined for all multiple choices and/or conditional tests/connections
- The function’s behaviour is predictable regardless of the incoming parameter,
- No buffer overflow can occur

Principle 8 – Hidden menus

Hidden areas should not access or modify areas related to executable code or sensitive data related to IMEI implementation.

Principle 9 – Prevention of substitution of hardware components

Hackers have been known to remove OTP components and replace them with other pre-programmed OTP components and this practice is economically viable for expensive handsets.

If no software anti-cloning mechanisms are implemented means should be implemented to prevent the substitution of hardware components containing memory and soldered on a printed circuit board.

Annex 1

This matrix may be used by manufacturers to indicate the dates by when they expect to be able to satisfy each principle and provide a brief comment if appropriate

Principle	Comment	Date Available
Principle 1 Uploading, downloading and storage of executable code and sensitive data related to the IMEI implementation		
Principle 2 Protection of components' executable code and sensitive data related to the IMEI implementation		
Principle 3 Protection against exchange of data/ software between devices		
Principle 4 Protection of executable code and sensitive data related to the IMEI implementation from external attacks		
Principle 5 Prevention of download of a previous software version		
Principle 6 Detection of, and response to, unauthorised tampering		
Principle 7 Software quality measures		
Principle 8 Hidden menus		
Principle 9 Prevention of substitution of hardware components		