EUROPEAN COMMISSION
ENTERPRISE DIRECTORATE-GENERAL

Conformity and standardisation, new approach, industries under new approach
Mechanical and electrical equipment (including telecom terminal equipment)
TCAM Secretariat

Anti-Theft Measures Mobile Phones

Status Report

Background

Some Member States are witnessing a steady, but alarming increase in the theft of mobile phones and related violence, to the extent that it is becoming a public order problem. Individual Member States are introducing legislation at national level to cope with the problem. Various measures have also been implemented to increase the security of the mobile phones and to discourage mobile theft. These measures have been proven to be only partially effective.

As the scale of the problem varies widely among EU Member States, not all EU public authorities are therefore addressing the issue. Some Member States requested the Commission to use article 3.3.d. of the R&TTE to resolve the issue on a European level. Directive 1999/5/EC foresees that the Commission may decide that equipment must support certain features ensuring avoidance of fraud. Some Member States see a harmonised EU solution as most desirable. Most Member States recognise the need for counter-measures for avoiding fraud and theft of mobile phones, within and beyond the EU.

The key questions to be answered are:

- Firstly, if the final solution will be found in enforced EU legislation or in voluntary industry initiatives;

- Secondly, which technology will provide the best means to avoid that phones can be used;

- Thirdly, if a European solution is enough to combat theft, as the issue of theft of mobile phones is a global problem.

In the future, the level of security of the terminals will become increasingly important when the mobile phones will also be used as payment terminals (e.g. financial transfers, mobile commerce) which will increase the value of terminals.

Current Industry and National measures and its effectiveness

- *Industry initiatives*

Various technical methods of securing mobile handsets have been implemented, such as the means to prevent the use of handsets after theft. Mobile operators have created databases to share blacklists of stolen terminals, based on the unique identity (International Mobile station Equipment Identity-IMEI). These databases are established on both national and international level (Central Equipment Identity Register-CEIR**)**. Stolen phones can be barred on all networks, by reference to the phone's unique identifying code (IMEI number). Operators can join this scheme on a voluntary basis.

Effectiveness

Operators: The IMEI numbers of many types can easily be reprogrammed. Very few operators register them in the databases, as they consider it time consuming, customer service unfriendly (call set-up time is delayed by checking the database, the wrong customer may be disconnected) and last but not least costly.

Manufacturers: Although IMEI numbers are used, each manufacturer uses differerent methods to make IMEI secure.

When regulated the testing of the integrity of the identity to conform with the R&TTE Directive would be the responsibility of the manufacturer. In the absence of standards, it may both be difficult for manufacturers to declare compliance as well as for public authorities to survey compliance.

It may be very costly to manufacture mobile phones if the identity of the phones could not be changed in both the hardware and software of the phones.

How can the effectivenessof IMEI based anti-theft systems be improved?

<u>Databases</u>

For the use of CEIR databases to become more effective the following measures may be required:

(1) all European operators (and their customers) register stolen phones to fight theft and fraudulent traffic, and

(2) all operators agree upon a uniform way of using the database, and

(3) manufacturers guarantee to continuously enhance and upgrade the security of the IMEI number whilst at the same time facilitating technological developments/progress under a uniform certification and security system.

Methods to secure the identity of the mobile phone

Although various methods exist to improve the security of the mobile phone, they should be evaluated for ease of implementation, effectiveness as an anti theft measure, cost effectiveness as well as their commercial feasibility for both manufacturers and operators.

Testing the security

Although methods exist for a manufacturer to enhance security by using common standards and certification, these methods require manufacturers, operators and others to co-operate to define suitable tests.

The testing of the security could be performed by independent third parties who will certify compliance with the agreed standards.

Manufacters and operators should agree and decide on these common standards and testing procedures for increasing the security in mobile phones.

- *National initiatives*

Some national EU authorities (UK/France) have introduced national legislation to combat theft of mobile phones. Amongst other things, such legislation provides for the following:

1. Enabling the police to tackle those fuelling the trade in stolen mobile phones with penalties (UK ‘Mobile Telephones Act’ up to 5 years prison) for one of the following reasons:

    - reprogramming the IMEI number
    - making it illegal to rewrite or change the software of the mobile phone
    - introducing extra hardware such as new memory or processors to change the identity and/or;

2. Forces manufacturers to take all technical measures possible to prevent the use of stolen mobile phones (e.g. by complying with –ETSI TS 122.016).

Effectiveness

No market data exist since these laws have been drafted. Their effectiveness is in practice hard to measure.

Discussions with the Industry and Member States

Discussions were held in recent meetings of the TCAM Committee (16/2/2002, 2/4/2003). GSM Europe has written to Commissioner Liikanen (December 2002) highlighting the need for the IMEI number to be regulated through the application of article 3.3.d of the R&TTE Directive. DG ENTR proposed a draft decision at the TCAM meeting in March 2003.

A workshop will be held on 3 June 2003 to hear and share views of all the stakeholders

(Member States, Operators, Manufacturers) on this topic. The objective of the workshop is to arrive at some common vision and clear steps forward for the stakeholders. Based on the outcome of the discussions , the Commission will decide, whether to formally proposo to Member States a decision to apply article 3.3.d.

The following questions will be addressed at the workshop:

1.What is the effectiveness of voluntary national and international industry initiatives?

2.What is the effectiveness of national Member State actions?

3.What kind of regulatory intervention at European level is necessary to secure the mobile phone security and what will the effectiveness of such measures be? Can it be implemented and what are the implications for all the stakeholders?

4. What are the technological methods to make the identity more secure? How can the security of the identity be tested (monitoring system)?

5. What is the most cost effective technological method for operators and manufacturers to optimise the security level of the identity of the mobile phone?

6. Is there a single solution that can address the challenge successfully?

7. How does a European solution create the basis for a global solution?

Possible conclusions

- Databases
  - National databases are ineffective as stolen handsets find their way across national borders. Databases must be linked and operators must be encouraged to register stolen phones. Solutions should be found for operator concerns.
- Technology
  - Developing new technology as a means to secure the identity of the handset, implies additional financial investments for manufacturers and operators. These investments will lead to higher prices and substantial investments are already done for the IMEI number, the industry should be heard on their proposals for further investment, and the effectiveness of such investments;
  - Manufacturers should be asked to continuously increase the level of security in the handsets and they should come with cost effective standards to do so;
  - Manufacturers and notify bodies should invest in methods to verify and certify security in handsets;
  - Manufacturers should be heard on security issues that could hamper innovation;
  - European co-operation is necessary between manufacturers, operators and public authorities to decide on the trade-offs in terms of technology, ease of implementation, cost effectiveness and regulatory.

- A more global solution may well be needed rather than just a European one

- Legislation should only be adapted or drafted once the full implication of such legislation is foreseen in terms of:

  - effectiveness of implementation

  - cost to the industry

  - possibility of enforcing the law

  - technology and standardisation

  - common standards for measuring

  - effect on future innovation by manufacturers