airwide solutions

Telecom Regulatory Authority of India

A Response to the Consultation Paper

Issues Relating to Blocking Lost / Stolen Mobile Handsets

Document version: 3
Document date: 30th November 2010
Reference: 30NOV10
Commercial in Confidence
Released

For more information on Airwide Solutions, visit our Web site:

http://www.airwidesolutions.com/

Every reasonable effort has been made to ensure the information and procedures detailed in this document are complete and accurate at the time of printing. However, information contained in this document is subject to change without notice.

Contents

1 Introduction

On November 2nd 2010, the Telecom Regulatory Authority of India published, in the interests of consumers, a consultation paper entitled 'Issues relating to blocking of IMEI for lost /stolen mobile handsets'.

Airwide Solutions, being a leading authority in the area of mobile network and device security, recognizes the fact that mobile handsets have become an increasing valuable part of consumers' everyday lives, and we are pleased to offer this response to the important questions raised in the consultation paper.

1.1 Abbreviations

Item	Definition
AMTA	Australian Mobile Telecommunications Association
CEIR	Central Equipment Identity Register
EIR	Equipment Identity Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

1.2 References

[1] Telecom Regulatory Authority of India Consultation Paper on Issues relating to blocking of IMEI for lost /stolen mobile handsets New Delhi: 2nd November, 2010

2 Response to Specific Issues

The following sections provide our response to the specific questions raised in the consultation paper.

2.1 Blocking IMEIs is an effective solution to Phone Theft

Question 1 'In order to reduce/discourage mobile theft do you think the blocking of IMEI is an effective solution? Please give reasons.'

Airwide Solutions believes that the blocking of IMEIs does act as an effective deterrent against phone theft, and that consumers, mobile operators and 3rd parties can all benefit from the provision of a CEIR. Specifically,

a) Consumers can benefit from blocking IMIEs because it removes the economic incentive for criminals to steal the owner's property in the first place. Indeed, whilst it is difficult to obtain police intelligence and accurate statistics on handset theft, it is interesting to note that within a few years, the AMTA was able to block over 250,000 devices in Australia alone. This represents a significant proportion of the estimated 200,000 devices lost or stolen in the country each year. (source www.AMTA.org.au)

b) Consumers can gain additional benefit from a CEIR, if selected 3rd parties are securely granted selective access to the CEIR database. For example, legitimate retailers of pre-owned devices would be able to check to see if a device has been stolen before selling on.

c) Although much has been written on the important emotional and economic impact of phone theft on the owner, it should be recognized that an operators' business can also be significantly impacted by such crime. This is because the loss or theft of handsets is often followed by one or more expensive customer care events. In fact, experience has shown that the theft of phones greatly increases the likelihood that an operator's affected pre-paid customers will move to a competitor's network

Apart from discouraging phone thefts, a central platform could also provide additional security functions related to the management of IMEI numbers. Hence, the regulator would be able to manage and control issues related to blank and illegal IMEI's, as well as cloned handsets. Optionally, they could also use the platform to provide basic fraud protection, and to generate international roamer statistics.

Finally, we believe the success in blocking devices using IMEIs can be recognized by the fact that a large number operators throughout the globe are now using the services of either a national or industry hosted CEIR, whether mandated by their government or not.

2.2 Minimizing the Load on the Network

Question 2. 'In case blocking of IMEI is implemented, to what extent load on the network will increase? Please give details'

In the case of blocking IMEIs, the load on an operator's network essentially originates from three processes:

a) Synchronizing the operator's own blacklist with that of the CEIR.

b) Updating the operator's EIRs with the new blacklisted devices.

c) Processing the checkIMEI requests from the network switches, to enforce the blocking of the handsets.

Each of these processes can be optimized to allow the service to be provided effectively, but without utilizing more than a minimal amount of network resources. For example, synchronizing the operator's local EIR blacklists with that of the CEIR would only need to take place once every 24 or 48 hours, and this could be timed to happen only during off-peak hours.

2.3 Managing a CEIR

Question 3) 'In your opinion, who should maintain the CEIR? Please give reasons.'

The CEIR implementation in India will be a unique one. It is apparent that the platform would have to be designed to keep in mind a need for additional security requirements as well as the functions discussed earlier. Hence, given the sensitive nature of the project, it is highly recommended that the CEIR be maintained by a technology provider party under the management, and with the close association, of the DOT. Such an approach would further facilitate a closer collaboration between the different operators serving the nation, and thus all would benefit from a service that would indeed be offered throughout India.

2.4 A CEIR Maintained at a National level

Question 4) 'Should the CEIR be maintained at national level or zonal level? Provide details including the estimated data size.'

A service maintained at a national level is recommended. This is because such an approach would be the most efficient, and cost effective, way of managing and sharing the blacklisted handset data across the country; something that would be especially needed to counter stolen handset trafficking across zones. This would also help better provide the other service features described above.

As regards to the calculation of the estimated data sizes involved, this obviously would be dependent on many different factors that remain as yet undecided. For example, the type and implementation of the database, the data stored in each record, the level of service uptake, as well as other operational considerations such as the service's data retention and purging policies, etc.

Moreover, we suggest that the system should also provide an efficient data redundancy capability, so that the service could be quickly resumed should a system outage occur. (The CEIR should certainly be designed such that an operator's principle business activities are not interrupted in the event of a CEIR failure.)

Airwide Solutions believes that a combination of the latest database technology with best in class EIR and data optimization techniques could deliver a cost effective system that would cater for the anticipated high rate of service adoption.

2.5 CEIR Costs & Funding

Question 5) 'Please comment on cost and funding aspects of Centralized EIR? Please provide detailed cost estimates?'

Detailed cost estimates could only be provided once agreement has been reached on the service's desired functionality, software / hardware requirements, and its operational support and development requirements.

We believe that the initiative would greatly benefit from sponsorship, and thus some form of ownership, from the Indian Government. Furthermore, the technology vendor and CEIR operator should be granted permission to generate revenue, within the purview of the existing regulations, by offering additional services to consumers, operators and approved 3rd parties. The income from such services could then be used to help fund the service.

2.6 Should Blocking of IMEIs / ESNs be Chargeable?

Question 6) 'Should blocking of IMEI /ESN be chargeable from customer? If yes, what should be the charge?'

We believe that the consumer should be able to have their stolen or lost phone blocked without having to pay a fee. This would be the best way to encourage the uptake of the service, and thus reduce phone theft. What's more, charging subscribers for blocking devices might actually cause customer dissatisfaction, and thus perhaps risk a rise in the operators' churn rates.

2.7 Legislation to Prevent Mobile Device Reprogramming

Question 7) 'Please give your views on bringing a legislation to prevent reprogramming of mobile devices? In your opinion what are the aspects that need to be covered under such legislation?'

Airwide Solutions agrees with the position taken by the GSMA; that governmental regulation of the industry's efforts to secure IMEIs would be impractical and consequently ineffective. We also agree that the self-regulatory efforts of the industry have gone way beyond that which could have been realistically achieved by governmental regulation.

However, legislative backed action, as outlined in the consultation paper, would be useful if directed against those who create, distribute and sell equipment and software that is used to unscrupulously change the IMEIs of stolen and lost phones. Such legislation could also serve as a deterrent for those who are considering offering IMEI changing services.

Where there is a legitimate reason to change a device's IMEI, this should be allowed but only with the express permission of the handset's manufacturer.

2.8 A Simple Procedure for IMEI Blocking

Question 8 ' What should be the procedure for blocking the IMEI?'

For the affected subscriber, the process for blocking an IMEI should be as simple as making a phone call.

Generally, the customer should be able to call a customer care number, have their IMEI / SIM numbers validated, their identity checked and their contact details recorded. The IMEI of their handset would then be distributed via the CEIR across the different operators as part of a blacklist, thereby blocking the device from use throughout the country. Following this, information can be collected on the blocked devices, to be shared in a secure manner to pre-approved 3rd parties.

In principle, the customer care call could be serviced by the operator, its approved agents or CEIR personnel. Obviously, there are different pros and cons to each route, and the process chosen would be depended on how (and what) information could be shared on behalf of the subscriber. However, it is clear that a centrally managed service could be beneficial in terms

of reducing costs for the operators, offering enhanced functionality, as well as increasing the overall efficiency of the process.

2.9 Unblocking the IMEIs from Recovered Devices

Question 9 'If a lost mobile is found, should there be a facility of unblocking the IMEI number? If yes, what should be the process for it? Should there be a time limit. Should it be chargeable?'

A mechanism to unblock the device should certainly be provided, so that the consumer can return to using their device to access the operator's services as quickly as possible. Failing to provide this facility would, in our opinion, inhibit service take up, generate consumer dissatisfaction and act as disincentive for operators wishing to join the service.

The process for unblocking the device would be essentially analogous to that already described for blocking a device. The onus, however, would be to on the subscriber to prove their identity and connection with the device. For example, after proving their identity, the subscriber could be asked to provide a unique case number given to them at the time they requested that their device be blocked.

Charging for unblocking a device may be acceptable to a subscriber, because they would have benefited from having their device protected (or even located) during the time it was out of their possession. This charge would not necessarily have to be very large. However, the price should be set at a level commensurate with the services provided, and to enable a meaningful income to be generated from the CEIR.

Finally, data should only be kept in the system for a pre-defined period of time, so as to protect the consumer's privacy and reduce the data management costs of the service. Whilst the IMEI should be barred for a long time, say 3 years from date of report, details of the consumer (if recorded) could be removed, for example, after 12 months.

Contact Details

Rajesh Khanna
Country Manager

Airwide Solutions
G1 - G2, Vipul Plaza,
Sun City, Sector 54,
Golf Course Road,Gurgaon 122002
Haryana - India
M: +91 98 104 49715
Email: Rajesh.Khanna@AirwideSolutions.com
www.airwidesolutions.com

Document history

Issue	Date	Change summary	Owner
1	19th November 2010	Initial document	JJ McChesney
2	29th November	Updated after Review	JJ McChesney
3	30th November	Final For Approval	JJ McChesney

Changes since last issue

Document control			
Owner:	JJ McChesney	**Title:**	Solutions Manager
Approved by:	R Khanna	**Title:**	Country Manager
Signature:	Approver signature	**Date:**	DD-Mmm-YY
Review record ref.:	File name	**Distribution:**	CTO, SVP SPM, VP SM
File name:	TRAI Response IMEI Blocking V03