



The Dynamics Of Introducing And Managing Mobile Broadband Within Developing Countries

– an interactive discussion.

Aircel India Limited

The 'Developing' Indicators

Penetration levels of fixed (wired) broadband subscriptions in developing countries remain low: 4.4 subs per 100 people compared to 24.6 in developed countries.

Business case for a Greenfield fixed line broadband deployment is also weak, even in highly developed and penetrated areas.

Most People in India use Handsets than PC to Access the Internet. Use of laptops/ PCs requires better network coverage and infrastructure, due to the much higher degree of indoor usage.

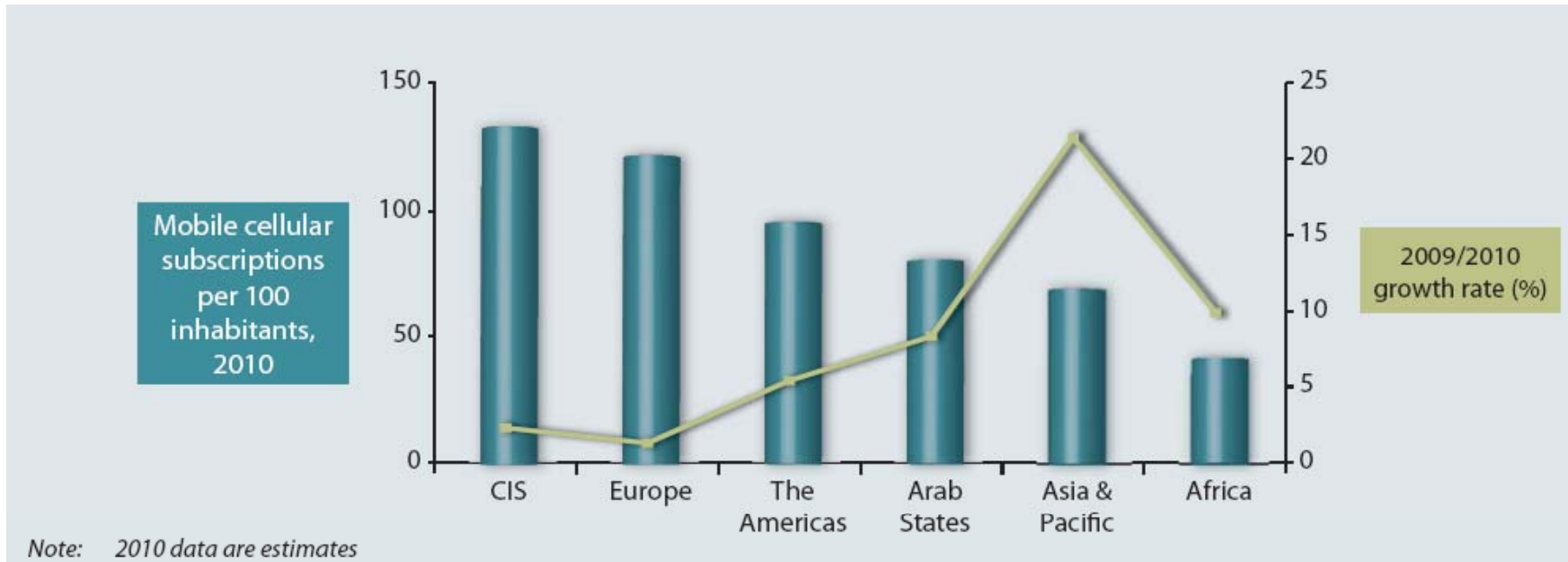
In Africa, it is a common practice to share one handset among many households.

Constraints in broadband usage in developing countries:

- Fixed Infrastructure like reliable power supply and wired connectivity
- Expensive access systems like computers/ laptops
- Low internet usage

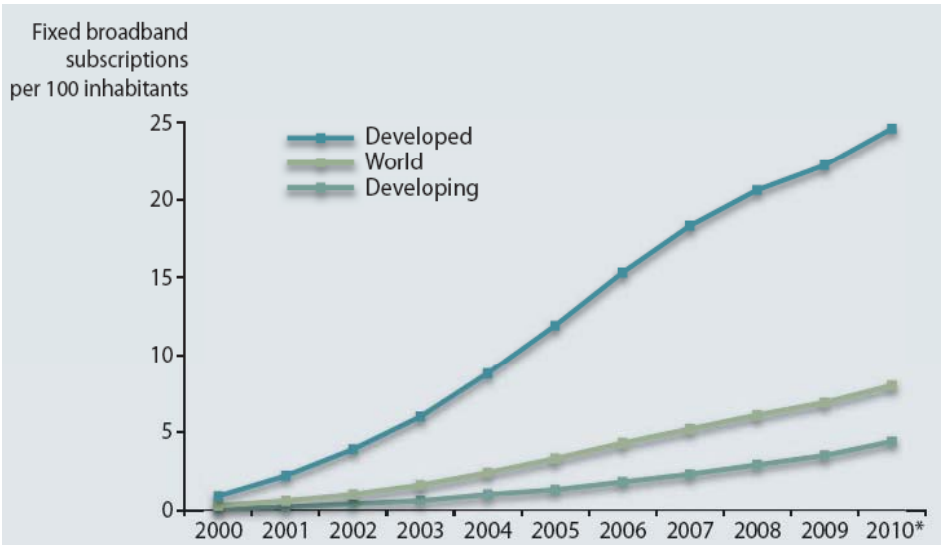


The Wireless World

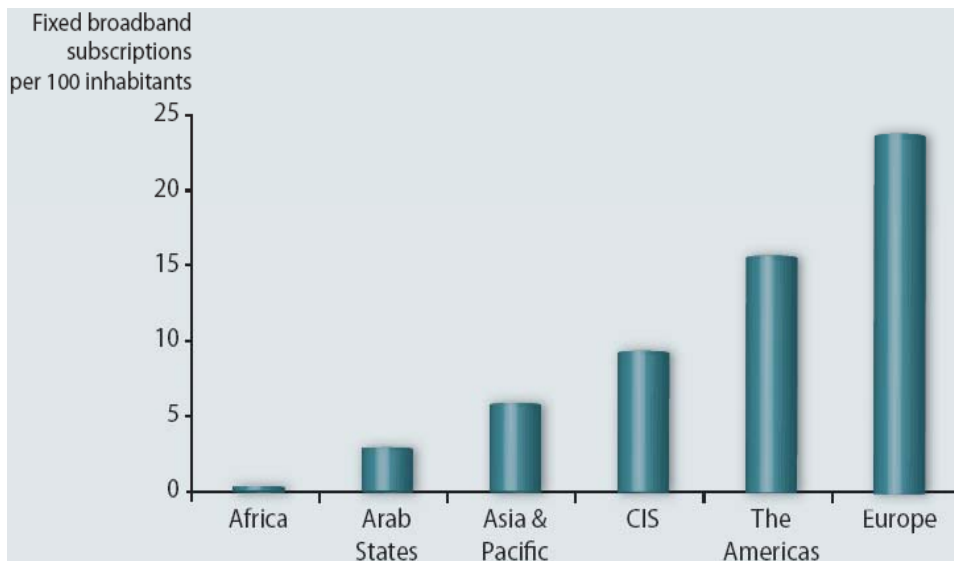


- In developed countries, mobile market is reaching saturation levels with on average 116 subscriptions per 100 inhabitants at the end of 2010, while the developing world is increasing its share of mobile subscriptions from 53% at the end of 2005 to 73% at the end of 2010.
- In the developing world, mobile cellular penetration rates will reach 68% at the end of 2010 - mainly driven by the Asia and Pacific region.
- India and China alone are expected to add over 300 million mobile subscriptions in 2010.
- In the African region, penetration rates will reach an estimated 41% at the end of 2010 (compared to 76% globally), leaving a significant potential for growth.

The Broadband divide

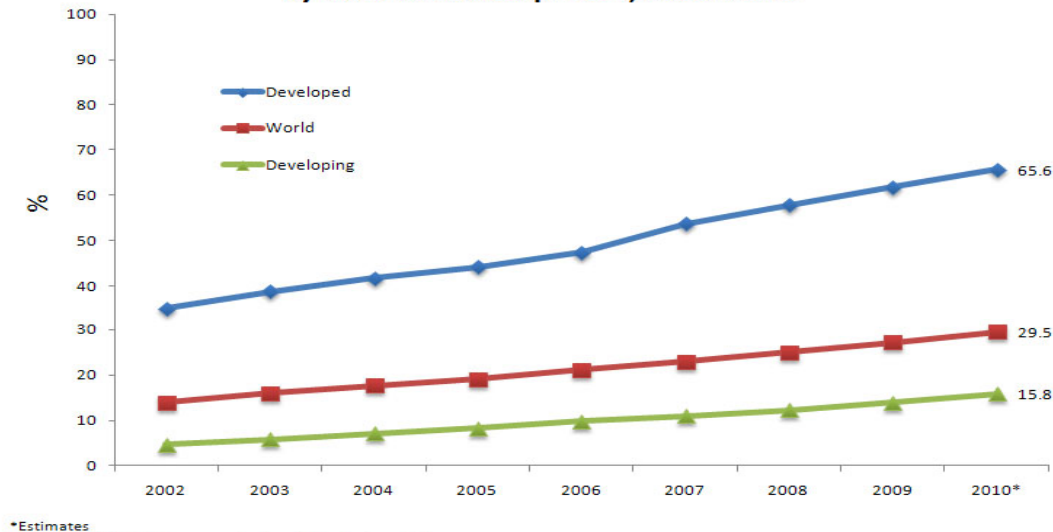


- Penetration levels of fixed (wired) broadband subscriptions in developing countries remain low: 4.4 subs per 100 people compared to 24.6 in developed countries.
- The developing world's share of fixed (wired) broadband subscriptions is growing steadily - by the end of 2010, the developing world will account for an estimated 45% of global subscriptions.
- Africa still lags behind with a penetration rate of less than 1% indicating the challenges that persist in increasing access to high-speed, high-capacity Internet access in the region.



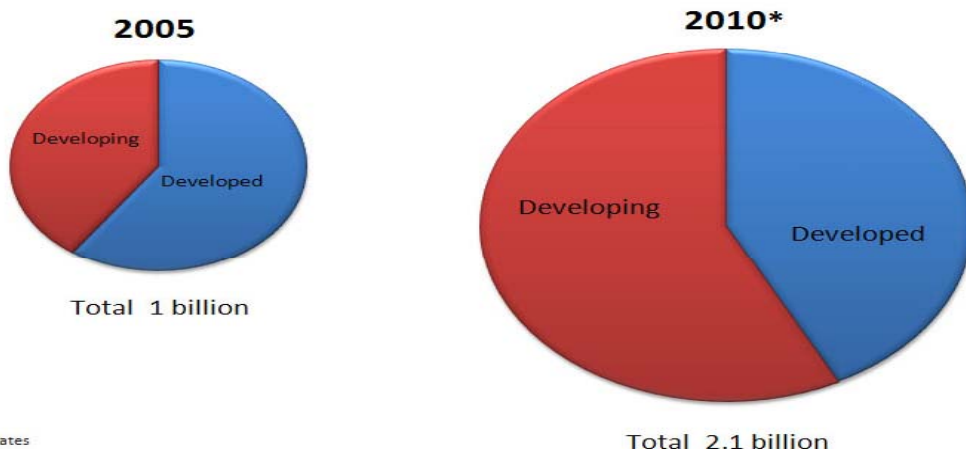
The WEB world

Proportion of households with Internet access by level of development, 2000-2010



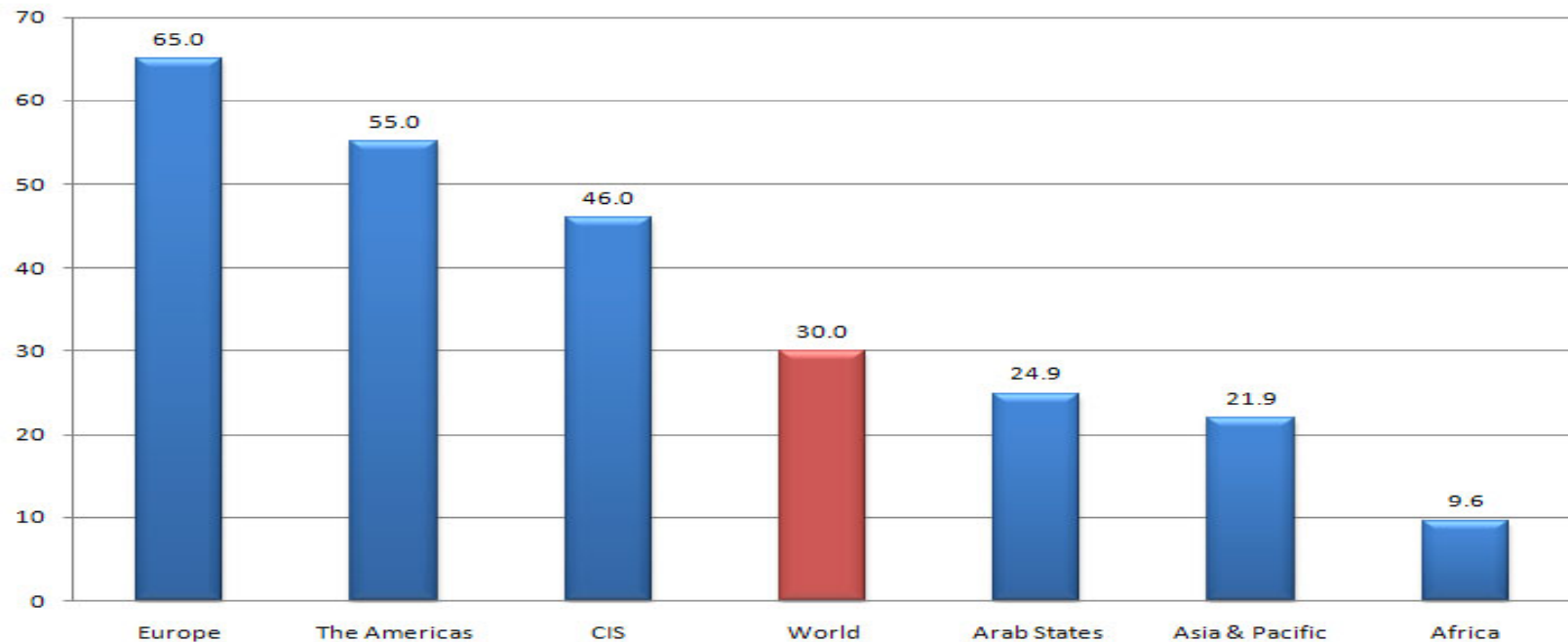
- The number of Internet users has doubled between 2005 and 2010.
- 71% of the population in developed countries are online, only 21% of the population in developing countries are online.
- In 2010, the number of Internet users will surpass the two billion mark, of which 1.2 billion will be in developing countries.

Internet users, by level of development



The WEB world

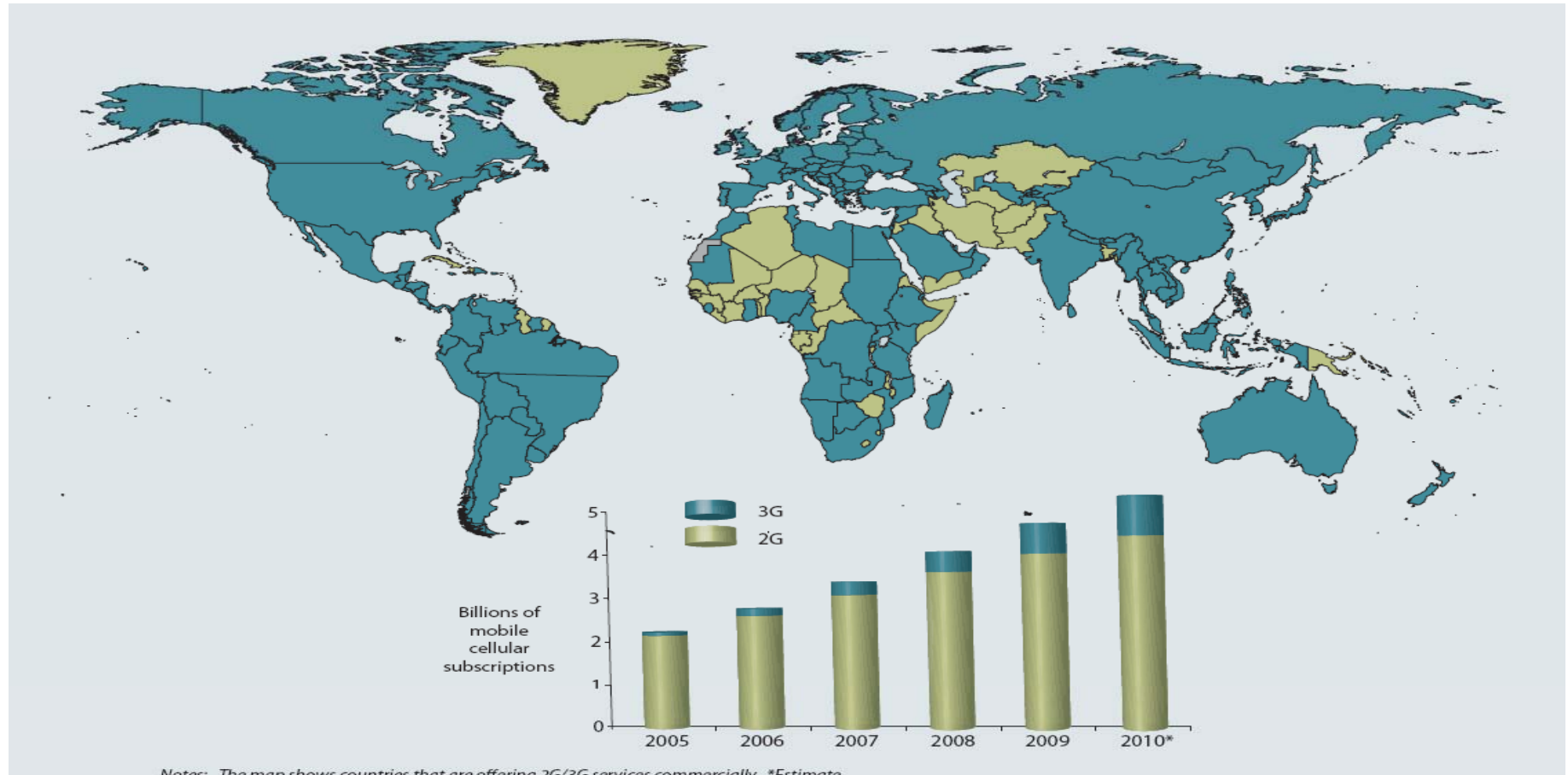
Internet users per 100 inhabitants, 2010*



* Estimate

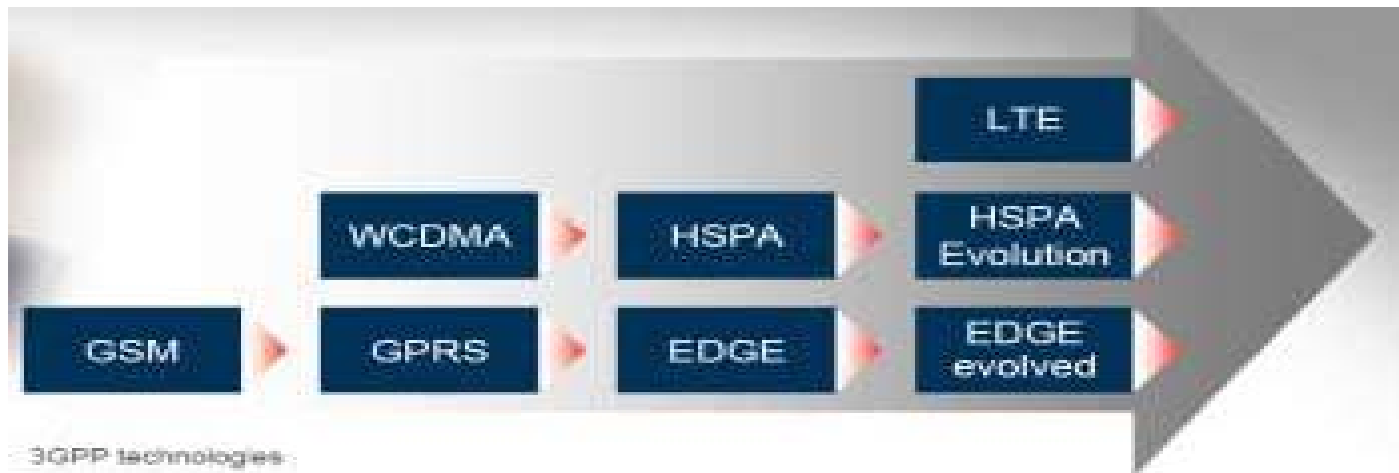
- By the end of 2010, Internet user penetration in Africa will reach 9.6%, far behind both the world average (30%) and the developing country average (21%).
- *Few **Developed countries**, including Estonia, Finland and Spain have declared access to the Internet as a legal right for citizens.*

Rise of 3G

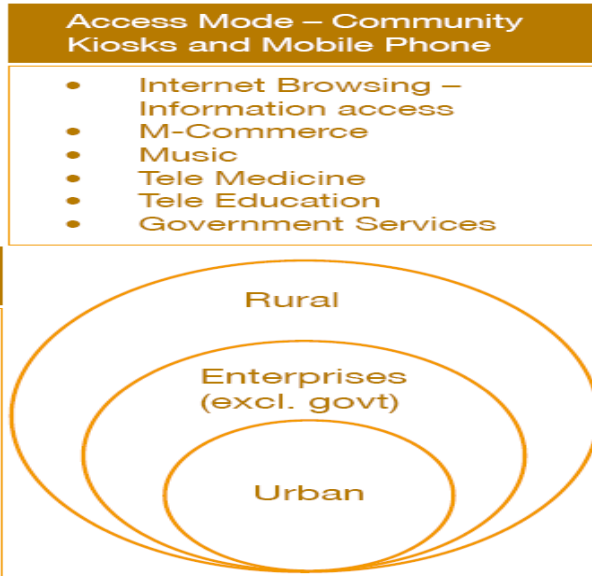


- By the end of 2010, there will be an estimated **5.3 billion mobile cellular subscriptions** worldwide, including **940 million subscriptions to 3G services**.
- Access to mobile networks is now available to 90% of the world population and 80% of the population living in rural areas.

The Wireless Evolution

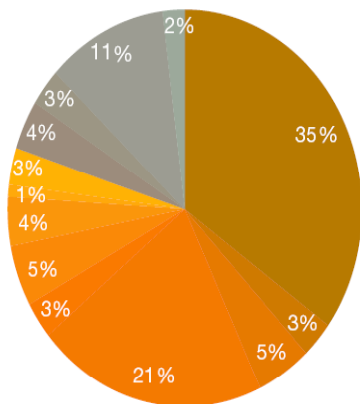


Early Applications of Mobile Broadband



- Access Mode – Mobile Phones, Dongles, Net books, Kiosks**
- Internet Browsing – Information access and Social Networking
 - M-Commerce
 - Video Calling
 - Music
 - Tele Medicine / Education Instant Messaging
 - Content Based Applications / Stores
 - Mobile TV

- Access Mode – Mobile Phones, Dongles, Net**
- Internet Browsing – Information access
 - Video Calling
 - Sales force Automation
 - Location Based Services
 - Mobility Services - Intranet & VPN
 - Net based Applications



- Internet browsing
- Mobile commerce
- Video calling
- Music services
- Video services
- Enterprise services
- TeleMedicine/ TeleEducation
- VOIP/Instant messaging
- Government services
- Location based services
- Gaming
- Application store
- Mobile TV

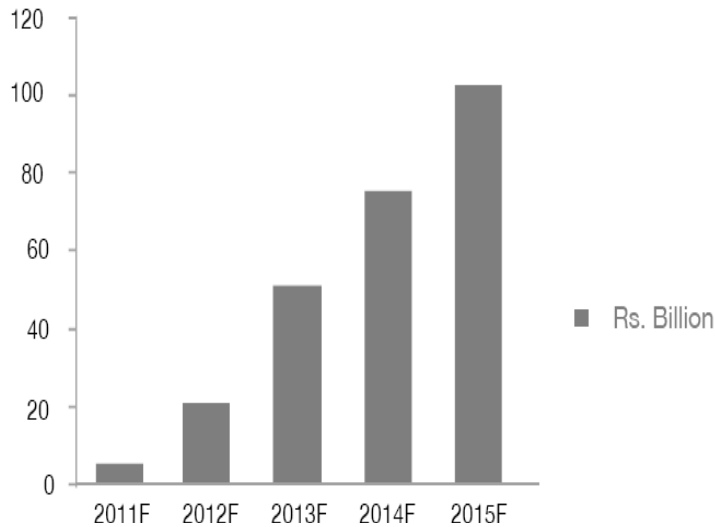
- Enabling Financial inclusion with Mobile based banking services.
- Media and Entertainment: Television, Music, Advertising, Mobile Gaming
- Agriculture: Farmers, Fishermen etc
- Transformation of Government Service Delivery
- IT and BPO services
- Internet browsing and music related applications would be the service drivers*



Indian Snap-shot: an indicative 'Developing' scenario



Incremental 3G data revenue



The increased data usage on 3G network will lead to incremental 3G data service revenue of over Rs. 100 billion in 2015 growing at 112 percent between 2011 and 2015.

3G mobile subscribers are expected to grow at 190 percent between 2011 and 2015, attributable to fall in the prices of 3G enabled handsets.

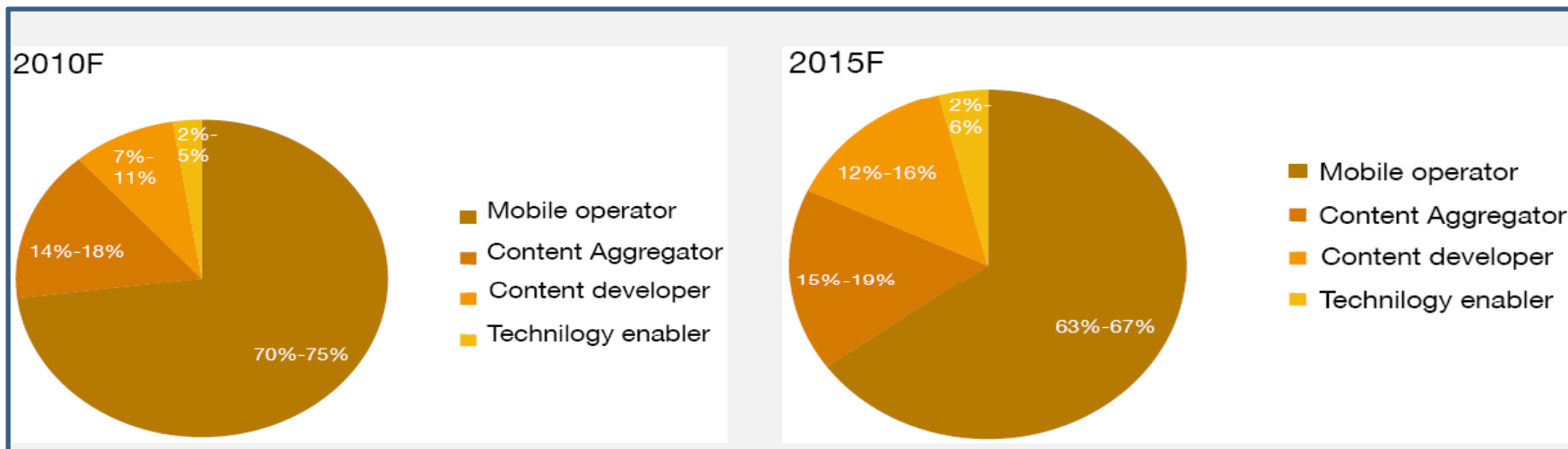
As content becomes the primary means to generate additional data revenue Telecoms' are expected to forego up to 10 percent of their share to VAS value chain players like content developer, aggregator and technology enablers by 2015

The incremental revenue for the telecom equipment vendors with the expected fresh contracts for 3G network roll out from the telecom operators. is expected to cross Rs.150 billion in 2015.

60,000 to 70,000 new employment opportunities are expected to be created by the telecom industry (service providers, handset vendors, equipment vendors and VAS value chain players) by 2015.

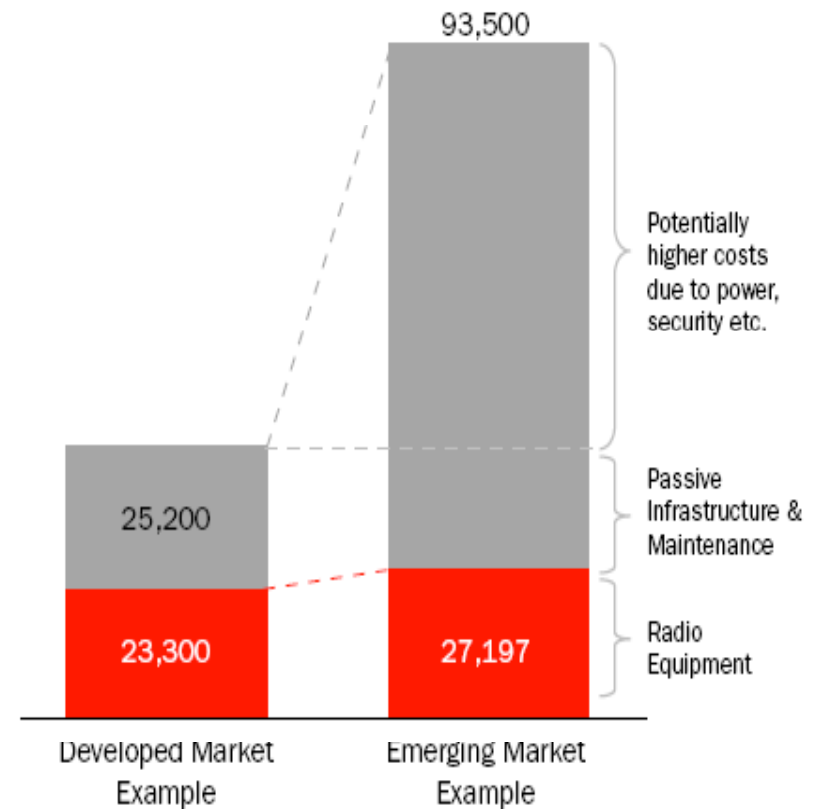
The total cumulative investment related to mobile broadband services is expected to be in the region of Rs 500 billion for the period of 2010-15.

Revenue share



Key Challenges for driving Mobile Broadband

- High Technology cost – largely dictated by infrastructure investments (see illustration)
- Adequate bandwidth for rich media mobile broadband services.
- Affordable 3G enabled handsets.
- Availability of utility and diverse vernacular content.
- Low levels of awareness & deployment of Wireless security practices & policies.
- Majority of mobile devices do not comply with government regulations or organizations' internal IT security policies, when exists.

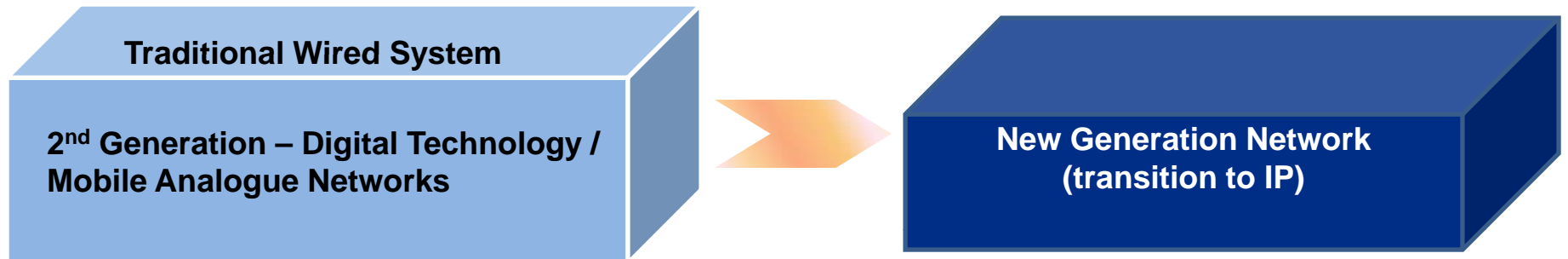


Mobile Operator Annual Network Cash Out per Base Station in 2007 -USD-

Evolution of Telephony Fraud



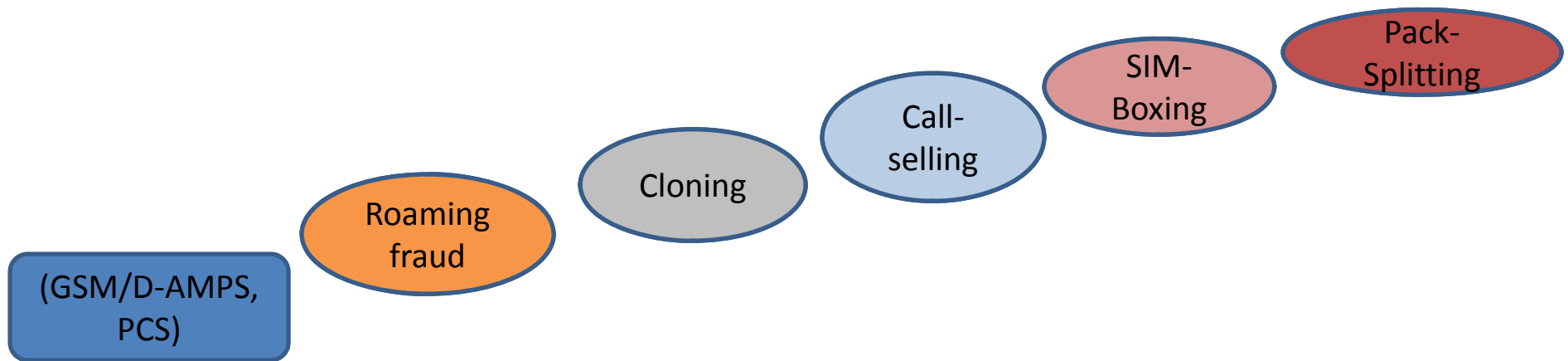
The Old Block.....



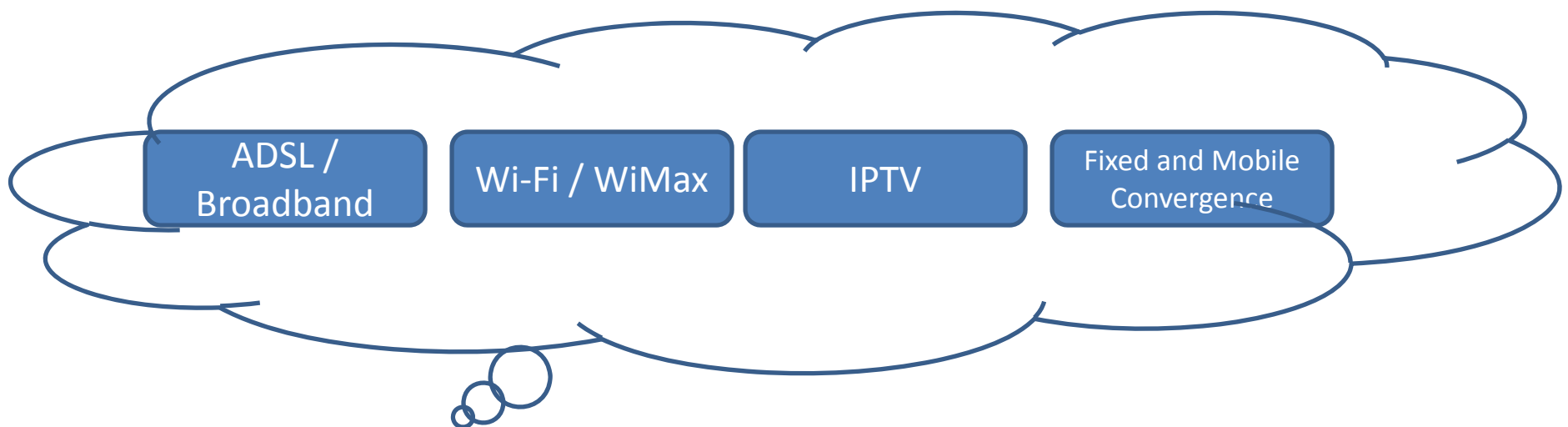
Wired telephone system		
Wire tapping	Account fraud	Multi colored box attacks

Evolution of Telephony Fraud

2nd Generation – Digital Technology / Mobile Analogue Networks



Emerging New Generation Network (transition to IP)



Emerging Fraud Threats...

Content Sell Fraud

The fraudster replicates and re-sells premium content, such as video or music les, at a fraction of the normal rate. This includes content resale (pirating) and IP infringement.

Content Artificial Inflation Fraud (AIT):

This is similar to traditional premium rate service (PRS) attack, but is increasingly associated with content downloads. It leaves the operator unable to collect fees from the fraudulent service use, but would be obliged to pay the content provider.

Click Fraud

In addition to content AIT, a specific type of internet-based fraud-commonly known as 'click fraud'. The fraudulent PRS content provider drives traffics to a paid content Website. This may be done manually, or by injecting phishing, malware to automatically use the service or hacking an operator's network to divert track to a content service, similar in nature to older auto-dialer attacks.

Crossover Fraud

Fraudster sends a "Trojan" to legitimate 3G subscribers. The Trojan causes the mobile devices of subscribers to automatically use service without the subscriber's authority or knowledge. This is commonly used to make premium rate calls that inflate revenues to the fraudster's own service.

IP Frauds

Networks adopting VoIP entice Hackers and criminals to capitalize on any weaknesses in the technology. VoIP is merely a transport protocol running on a data network which from a security viewpoint, is susceptible to all the attacks commonly targeted against data networks, even if they are not explicitly targeting voice over IP.

Malware

This general term applies to software that secretly installs viruses, key-loggers, etc - or malicious code executed on a computing device. It is another emerging fraud category that involves infecting devices with viruses and Trojans resulting in unauthorized actions. This might include making calls, deleting or stealing data. Once installed, unknown to the subscriber, a number of activities can take place, such as connections to PRS numbers, blocking calls, sending bulk SMS, or forcing legitimate services to fail.

Emerging Fraud Threats...

VoIP Bypass

This fraud involves diverting legitimate fixed-line or mobile originating voice traffic into VoIP sessions. This results in a loss of revenue for the terminating operator.

IP Spoofing

Use of IP spoofing (substitution of identity information) is the most common method, often to aid other frauds by offering anonymity to the fraudster.

Spamming/Phishing

Spamming and phishing refer to messages (usually randomly) sent out, typically to trick customers into disclosing credit card numbers, account passwords or banking information, or to prompt them to call a PRS service. Such e-mail/SMS/MMS messages often purport from spoofed mail address.

Spam over Internet Telephony (SPIT) consists of unsolicited bulk messages that are broadcast to phones connected to the VoIP WLAN network. Fraudsters send voice messages (such as PRS call-back or marketing spam) in bulk. Methods include hacking into a computer used to route VoIP calls to target a large number of subscribers.

Selective Phishing – aimed at a specific group of individuals such as key workers within a company who may be dealing with customer details or financial data

Broadcast Attack – aimed at anyone randomly selected from a large group of individuals.

Money laundering

With the increase in m-commerce applications, micro-payments, and e-wallet/purse implementations, many new opportunities are opening up for money laundering. For example, use of phishing type emails to recruit persons to help with money transfers i.e. messages to recruit financial couriers in order to transfer their funds from one world location to another. Money laundering may also be conducted in a virtual IP environment, although recent controls are making this much more difficult e.g. “Second Life” where Linden Dollars could be exchanged for actual currency allowing movement money.

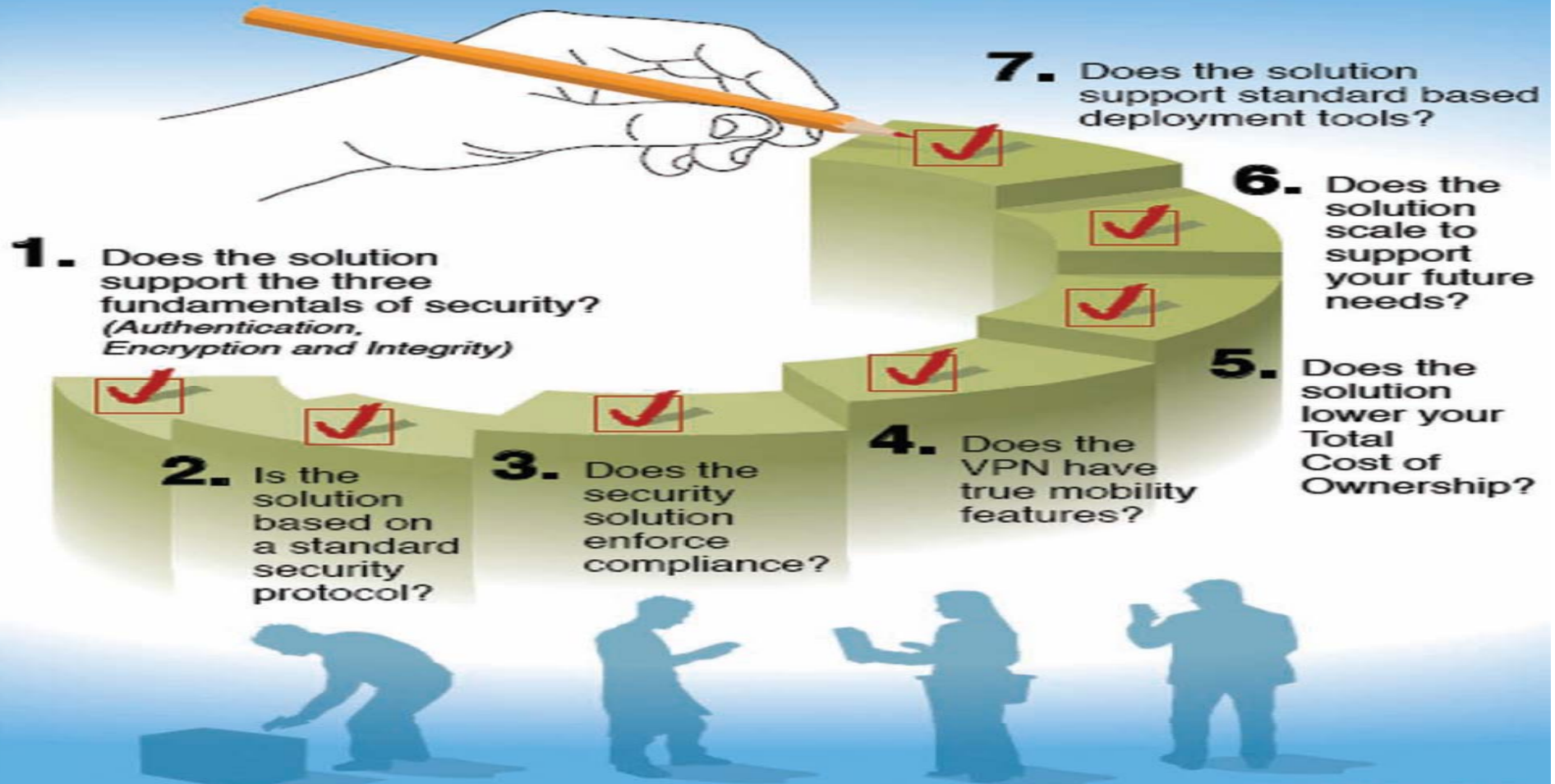
M-commerce related Frauds

Increasing opportunities and exploitation of m-commerce type services are opening the doors to Micro-payment frauds, including large-scale theft of (cheap) products, money laundering, and transaction denial. e.g. e-purse, wallet, or bank account (via banking application). M-Commerce could become more susceptible to fraud, due to tightening up of security and more attention to fraud threats being afforded in other Industry sectors (e.g. online retail).

Curbing telecom fraud



Your Checklist: Seven Steps to Secure and Seamless Field Mobility



Thank you

