

# GSMA Security Group Update

ETSI Security Workshop

16<sup>th</sup> January 2006

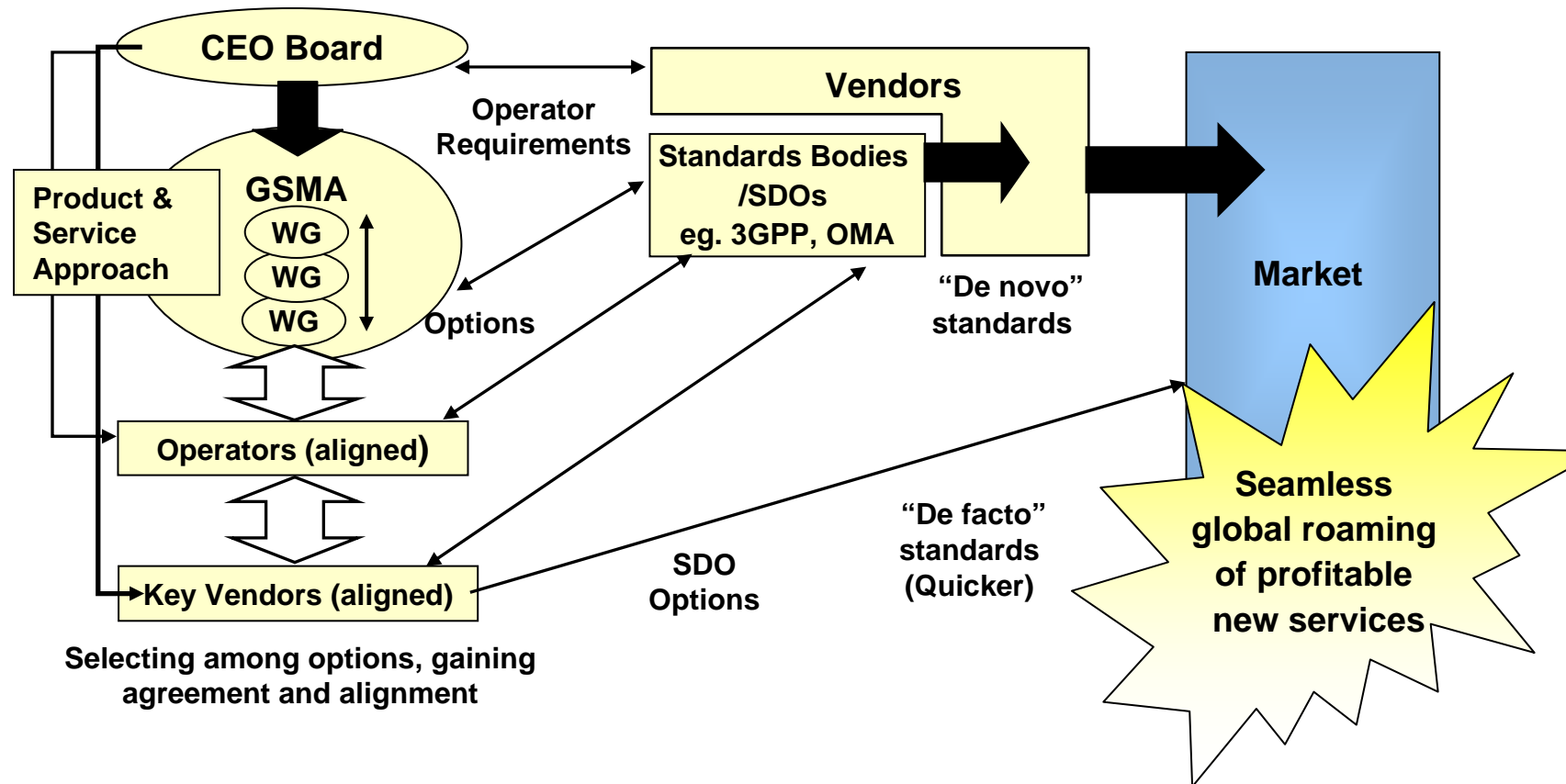


# GSM ASSOCIATION OVERVIEW

- World's largest and leading cellular trade association
  - 683 network operators in 212 countries
  - 150 key manufacturers and suppliers
- Objective is to arrive at a single voice on behalf of the operator community to establish building block requirements
- GSM serving 1.6 Billion customers globally
  - Took over a century for fixed line telephony to exceed 1Bn – GSM did it in less than 12 years
  - Global access – more people have access to GSM services than running water
  - More GSM handsets than PC and TVs combined
- \$500 Bn industry and GSMA is at the heart of it all

# GSMA Organisation

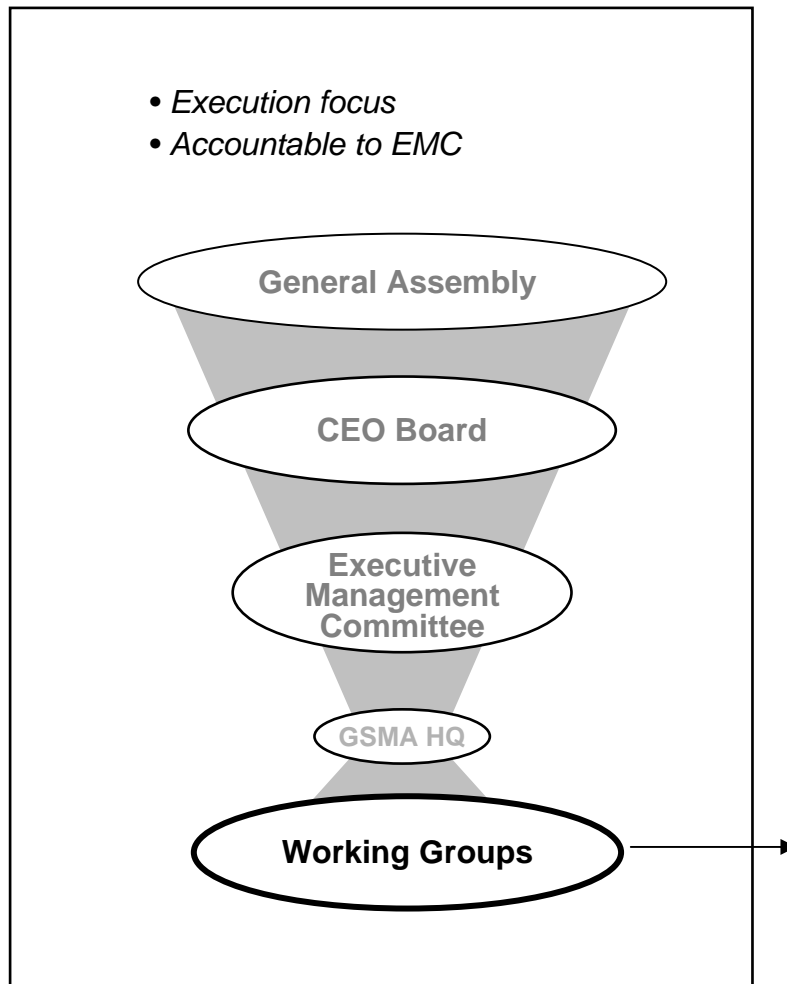
“Best route to market”



**GSMA - the best place to “accelerate implementation of collectively identified, commercially prioritised operator requirements”**

1. Ensures collective operators needs are met
2. Delivery of operator driven solutions derived from marketing requirements
3. Improved time to desired outcomes through moving at market speed

# Role of HQ and Working Groups



## Working Group high level description

### Composition:

- Operators and vendors provide content expertise for Working Groups and Special Project Teams
- GSMA provides project and programme management support

### Responsibility:

#### Execution

- Delivery of prioritised activities
- Contribution to Special Project Team initiatives

#### Education

- Facilitate education of attending delegates
- Meeting management
- InfoCentre documentation availability

### Reporting

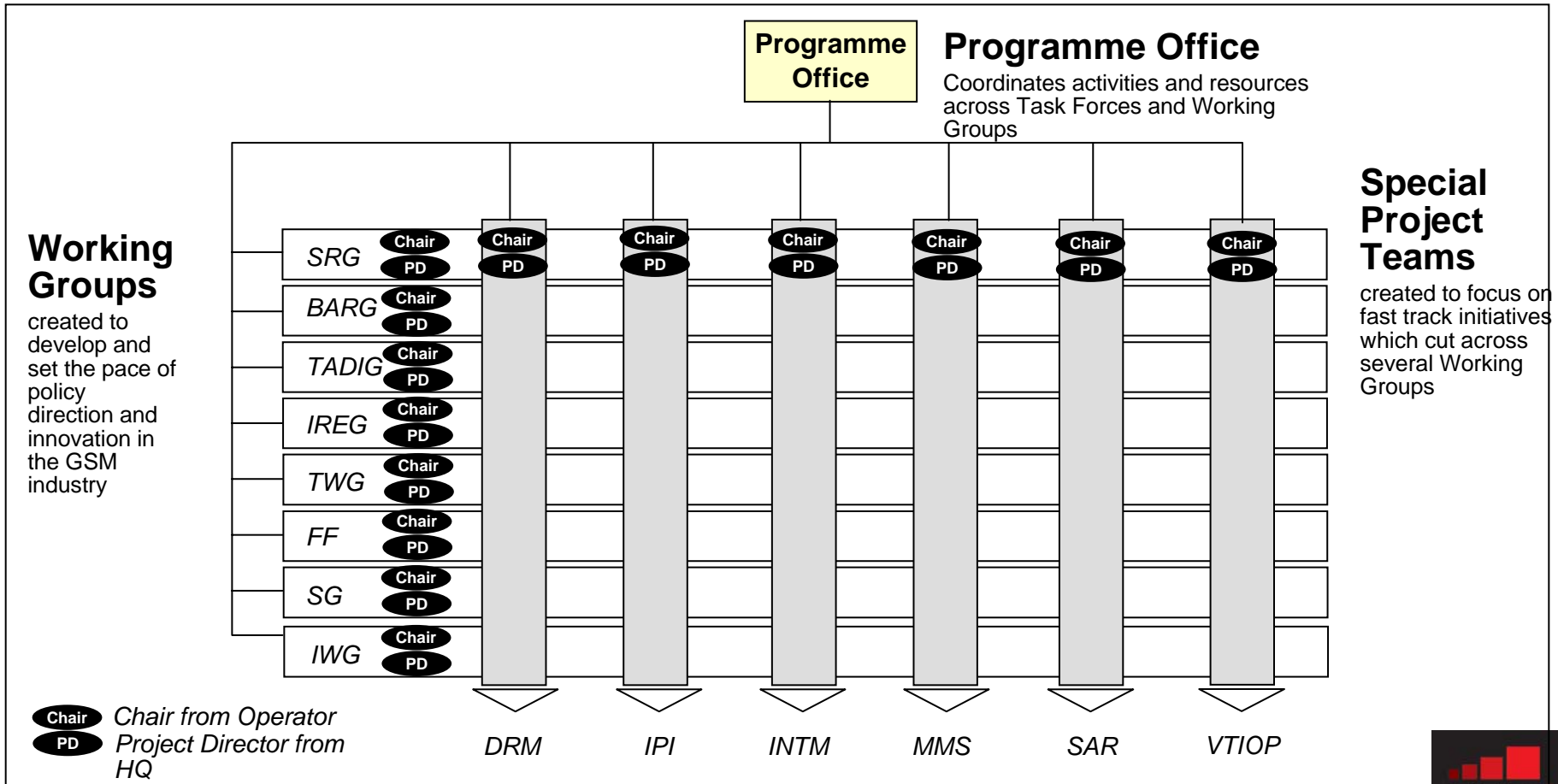
- Working Groups and Task Forces report to EMC

### Time Commitment

- Varies by role – 5 to 10% % generally sufficient

# GSMA Execution Model

## The Execution Matrix – Task Forces and Working Groups



# Security Group - What is it?

- Oldest working group - Est 1989
- Specified security protocols for GSM - the most secure mobile standard
- Partners with 3GPP TSG SA3 and ETSI SAGE
- Chairman is Charles Brookson, DTI
- 4 meetings per year with 1 annual joint meeting with FF
- GSM 2000 joint project team with ETSI/3GPP TSG SA3
- Average attendance of 30 delegates



# Terms of Reference

- Identify and analyse security risks to which network operators are exposed
- Advise network operators of the latest best practice being adopted in terms of technical security
- Maintain and develop security algorithms and protocols
- Apply and maintain technical security aspects of customer apparatus and network infrastructure
- Submit operator requirements to international standards bodies
- Advise on technical solutions to combat fraud

# Overall Objectives

- Maintain the level of technical security of GSM
  - Network security
  - Customer security
- Improve level of security
  - New algorithms (A5/1, /2, /3 – Comp 128-1, -2, -3 and G Milenage)
- Meet changing threats

# Challenges

- Ignorance and indifference
  - Some operators not ciphering or authenticating
  - Handset theft issue not clearly understood
- Security functions and responsibilities are fractured within operators
- Products and Services introduced with no security input or consideration
- ***Security is not important until something happens to me.....***
- There are financial and business implications – security is an enabler
  - Do it well at less than 0.5% of turnover loss
  - Do it badly, we have seen losses of > 60%



# PRDs

- **SG.01 – 04**
  - Distribution rules and NDA's pertaining to algorithms
- **SG.07**
  - Threat Analysis of the GSM System
- **SG.09**
  - Interception Requirements
- **SG.11**
  - Frequently Asked Questions and Answers
- **SG.14**
  - Operations and Maintenance Access Control
- **SG.15**
  - Operator Guidance on the use of Security Mechanisms
- **SG.16**
  - Security Advice to GPRS Users
- **SG.18**
  - Functional description of CEIR

# Past success

- Regular algorithm improvements
- False base station attack solutions
- Lawful interception as a 'standard'
- Handling press comments and speculation
- PRDs for securing networks
- New IMEI Database and the IMEI
- SIM Security Accreditation Scheme
- 3G standardisation influence
- Security reviews carried out on the following services:
  - WLAN
  - MMS
  - Root DNS
  - Push to Talk Over Cellular

# 2005 SG Work items

- Industry communications and documentation updates pertaining to withdrawal of A5/2
- Administrative arrangements and development of new UMTS cipher algorithm progressed
- Definition of minimum requirements/guidelines for vendors regarding anti-spam functionality
- Requirements identified to develop a CERT like service dedicated to wireless security issues and proposal drafted
- Handbook produced for operators providing guidance on security issues related to the migration from 2G to 3G
- Monitored handset manufacturer compliance with implementation of March 2004 industry agreed handset security initiatives
- Definition of elementary tests to evidence implementation of defined minimum security levels across all networks

# 2006 SG Work items

- Oversee and Monitor Network Operator Swap out of A5/2
- Commence Distribution of New UMTS Cipher Algorithm
- Wireless Emergency Response Team Service to reduce exposure to security attacks/vulnerabilities GPRS
- Development of Secure Use of Mobile Phones Public Information Portal
- Legal framework to sanction mobile virus writers
- Secure migration from IPv4 to IPv6
- GPRS Immediate Service Termination

# GSMA Security Services

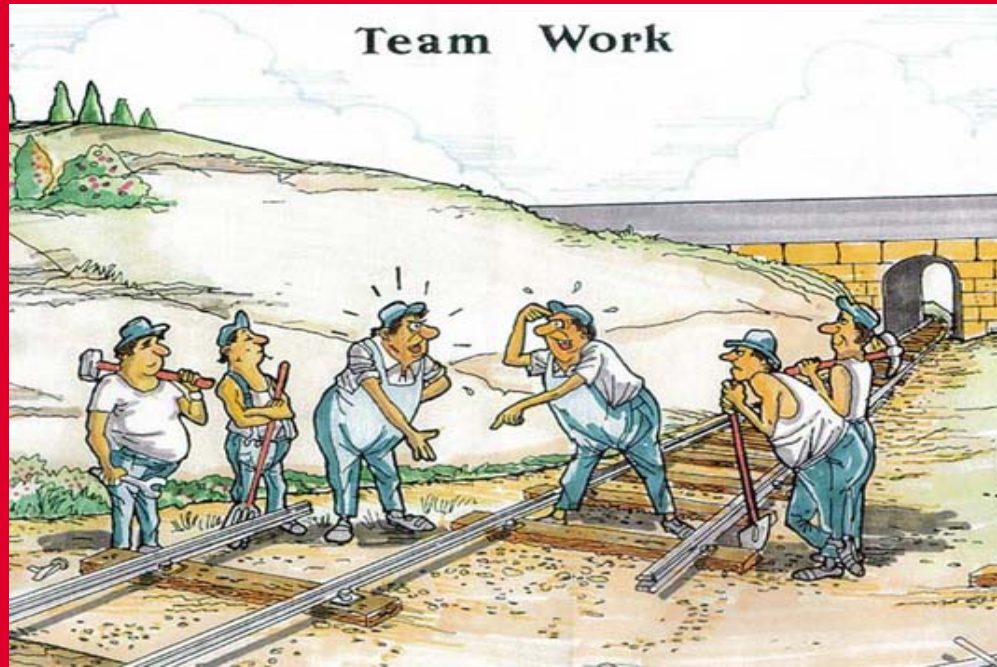
- Algorithm distribution services
- Fraud and security advisory service
- Support and project management
- Document and online content maintenance
- Security Accreditation Scheme
- GSMA fraud training programme
- IMEI Database
- Monitoring and reporting on handset theft

# Finally.....

- SG has added significant value and has strategically contributed to many GSMA initiatives and industry successes
- SG is a working group ... it is also a forum where operators can share experiences and incident reports
- It can't do either without the necessary resources

**SG welcomes contribution and, in particular, it requires IP expertise to deal with emerging issues**

**Collaborative efforts can continue to be effective ...  
they just need to be aligned!**



**Thank you for your attention**

James Moran  
Fraud and Security Director  
GSMA Association  
jmoran@gsm.org