ETSI EMTEL

(Special Committee on Emergency Communications)
CHAIRMAN Ray Forbes

Producing and maintaining Standards for Emergency Communications

Presented by Ian Harris
EMTEL Vice Chairman
Consultant to Research In Motion

Standards for Business

What are Emergency Telecommunications

- Emergency telecommunications covers all communication services, including voice and non-voice, data, location etc…
- The need for emergency telecommunications includes many scenarios ranging from:
  - a minor road traffic accident, for example
  - to a major incident like a passenger train crash, a terrorist incident, a natural disaster (e.g. an Earthquake, Tsunami).
- Provision for emergency telecommunications is also a major requirement in disaster situations

History of SC EMTEL

- EMTEL was previously OCG EMTEL: ETSI Board created an ad hoc group for coordination of Emergency Telecommunication activities

- Then the group became Special Committee (SC) EMTEL:
  - It was created and approved by Board#50 in February 2005
  - SC EMTEL reports directly to the ETSI Board

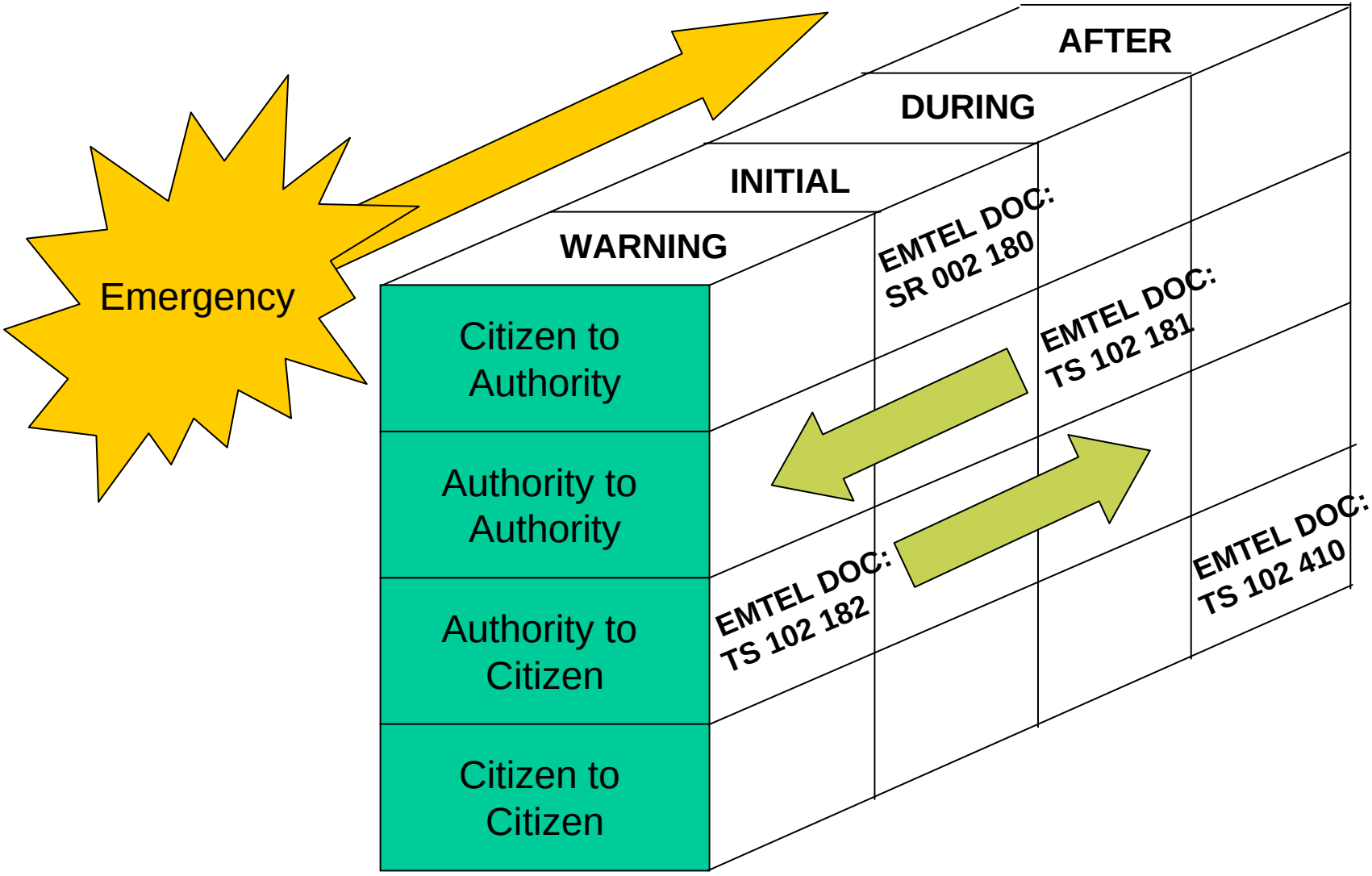
Main responsibilities of EMTEL

- Act as a key coordinator in getting requirements on Emergency Communications, outside ETSI (i.e. from different stakeholders) and inside ETSI (i.e. ETSI Bodies).
- Provide requirements on issues of network security, network integrity, network behavior in emergency situations, and emergency telecommunications needs in networks
- Co-ordinate the ETSI positions on EMTEL related issues
- Be the Interface for emergency communications issues
  - between ETSI
  - and CEC/EFTA, NATO, ITU groups, the CEPT ERO and relevant CEN and CENELEC committees

User requirements and scenarios

- The requirements are collected to ensure:
  - Communication of citizens with authorities
  - Communication from authorities to citizens
  - Communication between authorities
  - Communication amongst citizens
- Generally agreed categories to be considered in the provision of emergency communications for practically all types of scenario
  - Including communications resilience and network preparedness

Document Structure of EMTEL



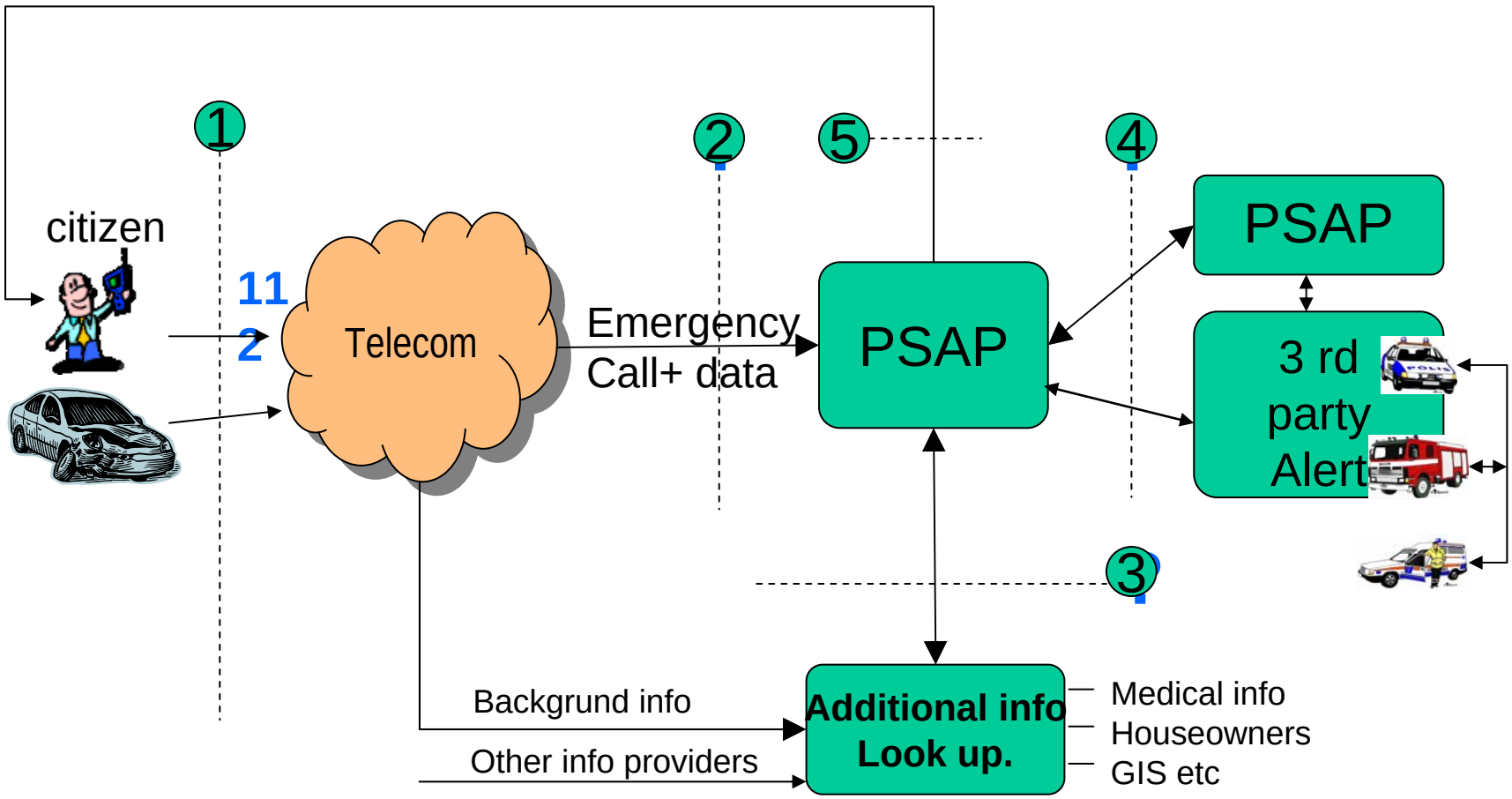
Fixed or Mobile technology?

- Communication for: Citizen to Authority', 'Authority to Citizen' and 'Citizen to Citizen' for Voice and data service from both wireless and wireline access (including normadicity on fixed line users)
- Public broadcast services (often used also): in support of 'Authority to Citizen' communications
- Both fixed and mobile technologies: for 'Authority to Authority' communications utilized by public safety organizations in Europe already (same technologies as those used for routine public safety telecommunications)

Private or Public networks?

- Telecommunication technologies used for emergency telecommunications are often no different than those used for routine public safety telecommunications
- Sharing of networks with non-public safety users is commonplace
- Wireless technologies are likely to be combination of narrowband, wideband and broadband, and nature of application use public or private networks
  - Public: GPRS and 2/3G
  - Private: Wideband TEDS and Broadband PPDR
- Migration toward IP technologies the private access mobility & nomadicity between public and private access will be common
- A combination of both proprietary and ETSI telecommunication technologies are often used

Interfaces needed to access emergency services

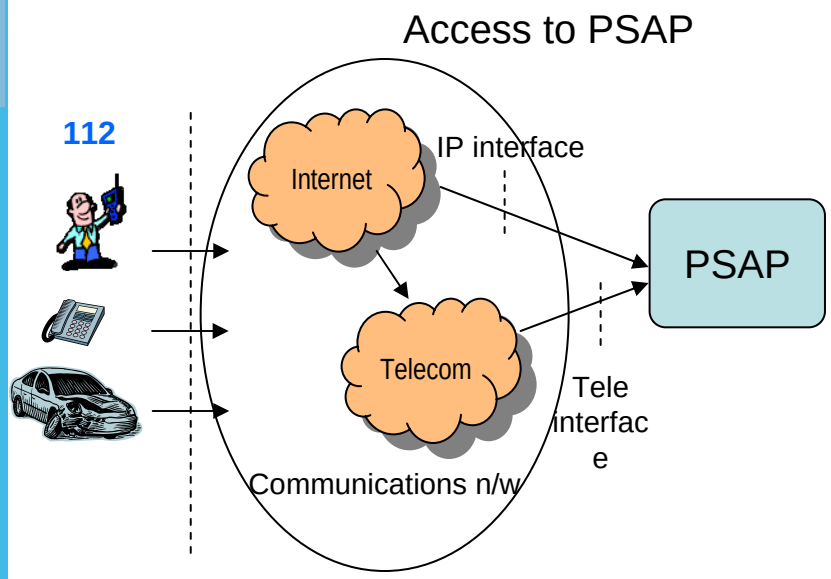


1. Citizens emergency call to authority/ PSAP
2. PSAP Required Information related to 112 call
3. Other data information
4. Authority to Authority
5. Authority to citizen

Standards for Business

Requirements and standardisation

The roles of different groups



Expert Group on Emergency Access

COCOM subgroup

- High level operational requirements
- Defines mandatory and optional requirements

EMTEL

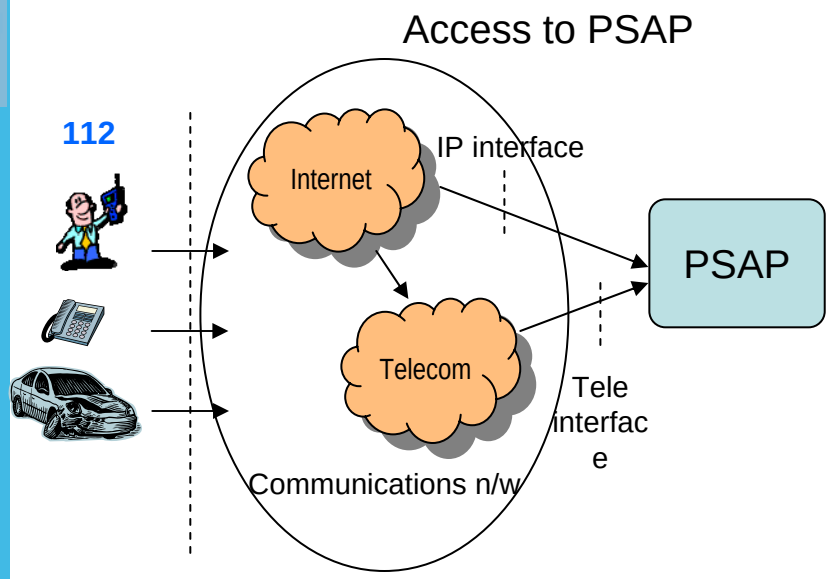
- Functional requirements (models)
- Elaborates the specification of functions

Technical bodies (ETSI other groups, 3GPP, IETF etc.)

- Technical standards (implementation)
- Works out possible solutions

Requirements and standardisation

Examples today



Expert Group on Emergency Access

COCOM subgroup

- High level requirements: Identification of caller
- Defines mandatory and optional requirements

EMTEL

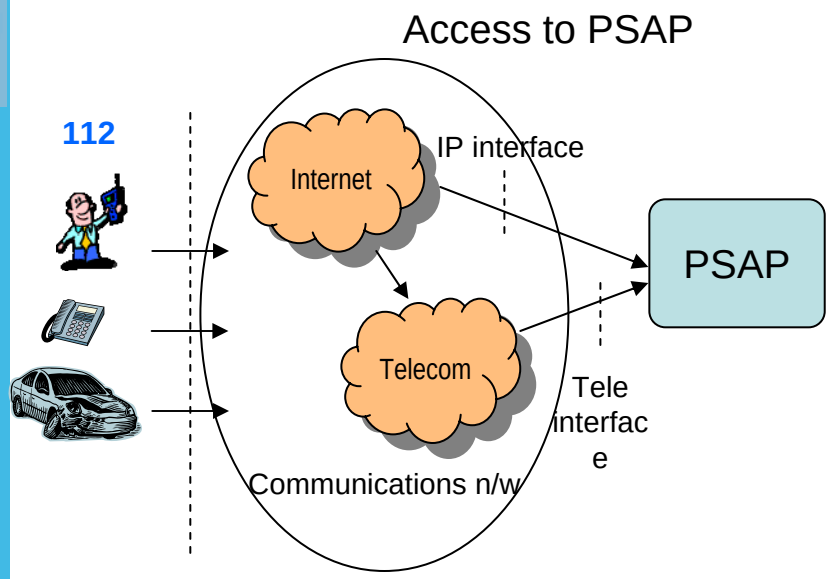
- Functional requirements: Can be A-number and/or..
- Elaborates the specification of functions

Technical bodies (ETSI other groups, 3GPP, IETF etc.)

- Technical standards: Transferred in ISUP, PABX-signalling, exact format etc.
- Works out possible solutions

Requirements and standardisation

How should TR 102 476, EC and VoIP be read



Expert Group on Emergency Access

COCOM subgroup

- High level requirements: What call cases should be supported concerning routing, identification and location of VoIP

EMTEL TR 102 476

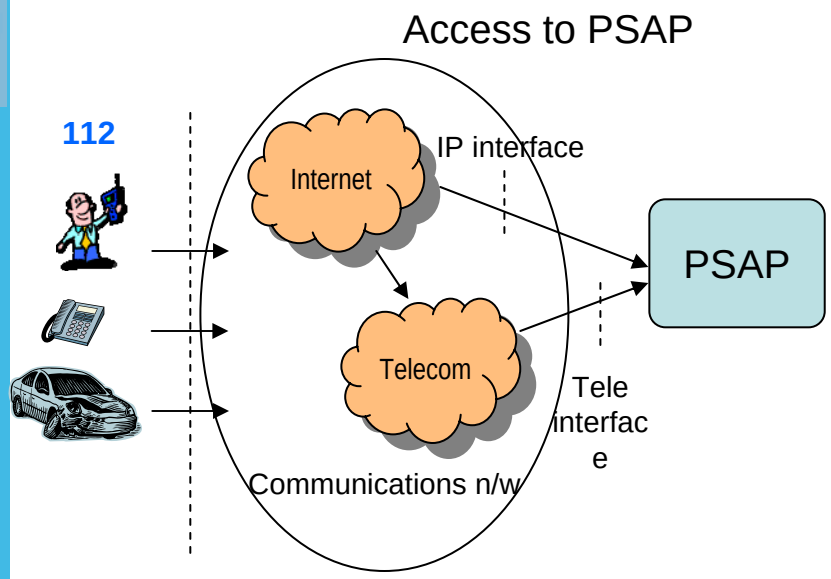
- Description of different possible methods to functionally implement this.
- Identification of need for standardisation

Technical bodies (ETSI other groups, 3GPP, IETF etc.)

- The technical solutions that are possible

Requirements and standardisation

Examples concerning VoIP



Expert Group on Emergency Access

COCOM subgroup

- **High level requirements: Routing to ”right” PSAP**

EMTEL

- **Functional requirements: What is ”right” PSAP**

Technical bodies (ETSI other groups, 3GPP, IETF etc.)

- **Technical standards: Solutions to find ”right” PSAP e.g. DNI-request**

EMTEL ETSI published deliverables

- SR 002 299: Collection of European Regulatory principles (may be revised to add PATS Regulation for ECNs)
  Published in April 2004

- TS 102 181: Requirements for communication between authorities/organizations during emergencies
  Published in December 2005

- TR 102 444: Suitability of SMS and CBS (Cell Broadcast Service) for Emergency Messaging
  Published in March 2006

EMTEL published deliverables in revision

- TR 102 182: Requirements for communication from authorities to citizens during emergencies
  Re-approved as TS 102 182 in September 2006
  Revised and up issued to a Technical Specification to include parameterisation of the alerting requirements

- SR 002 180: Requirements for communication of citizens with authorities in case of distress (emergency call handling)
  Reopened in April 2006
  Revised to include requirements for VoIP and Sip based Emergency and location services, capturing these requirements in a technology neutral way will also be considered

- TS 102 181: Requirements for communication between authorities/organizations during emergencies
  Reopened in September 2006
  Reopened for consideration of inputs from ETSI TETRA

EMTEL ongoing deliverables

- **TR 102 445: Requirements for Emergency Communications Network Resiliency and Preparedness**
  Approved September 2006

- **TR 102 410: Requirements for communication between citizens during emergencies**
  Stable in September 2006

- **TR 102 476: Technical Report was created: Study of Emergency calls and VoIP**
  Stable in September 2006

EMTEL matters in other ETSI Bodies

- Although SC EMTEL was formed to specifically address public safety user requirements for Emergency Telecommunications, other Technical Bodies (TBs) within ETSI have been active for some time:
  - Activity co-operating between 3GPP and ETSI TISPAN on the specification of a Mobile Location Positioning protocol for the delivery to the Emergency Authority the position of a caller to the Emergency Services
  - ETSI TISPAN has approved the Emergency requirements for NGN Systems
  - The definition of a SIP interface from the NGN system toward a PSAP may be under consideration, clarification of the need for this so called peer-to-peer sip interface is sought from the EU commission and PSAP Operators.
- Many standards related to EMTEL topics (more than 700) are developed by other ETSI Bodies i.e. 3GPP, TC TISPAN, EP MESA, TC TETRA and TC ERM

EMTEL matters in other ETSI Bodies

- You can find the main standards on the EMTEL Status Report page (ETSI Portal): http://portal.etsi.org/emtel/status.asp
- And for more details have a look at the ETSI Work Programme, advanced search, by selecting the project code EMTEL: http://webapp.etsi.org/WorkProgram/Expert/QueryForm.asp
- Liaisons are regularly exchanged with other ETSI Bodies

Co-operation with external Bodies

- A Memorandum of Understanding has been signed between ETSI and NENA (National Emergency Number Association) end of 2005, involving mainly EMTEL and TISPAN
- Regular liaisons are exchanged with TIA, ITU-T, NATO
- ETSI and NATO are co-sponsoring a Civil Military Co-operation (CIMIC) workshop in September 2006 to look at how best provide communications at major incident/disaster scenarios
- Informal liaison on USA initiatives – EAS (Emergency Alert Service) and WARN (Warning Alert and Response Network)
- Informal liaison on Japanese Earthquake Warning System

Cooperation with EU Projects

- EMTEL is involved in EU Projects
  - eCall project (in-vehicle automatic emergency call), project required by the Commission to ETSI
  - In co-ordination with TC MSG (Mobile Standards Group), TC ERM TG37 (Intelligent Transport Systems) and TC TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks)
  - TC MSG eCall agrees that the documentation of the eCall requirements will be discussed in 3GPP. eCall MoU Driving group has now held their final meeting.

Contact EMTEL

- Next EMTEL Meeting: 30th October-2nd November 2006 in St. Paul de Vence Nice, France.
- For more details you can:
  - Visit our ETSI EMTEL Portal: http://portal.etsi.org/portal_common/home.asp?tbkey1=EMTEL
  - Browse the ETSI EMTEL Web site: www.emtel.etsi.org
- Don't hesitate to contact the Chairman at: raymond.forbes@marconi.com
- Or emtelsupport@etsi.org

National Emergency Message Broadcast Challenges

- **Location specific**
  - Emergency message may only be relevant for a certain area.
- **Language**
  - Emergency message may need to be sent in different languages in the same country for visitors and non nationals. More of an authority challenge than technical.
- **Timeliness**
  - Studies have shown that ‘seconds count’ for some disasters such as Earthquakes and Tsunamis.
  - Implications for transport technology and the receiving device. Speed of delivery and recipient interaction.
- **Message content**
  - May need to contain warning *and* instruction.
- **Authentication**
  - Essential to avoid false / malicious alarms.
- **Cost**

Possible Mobile Technologies

- Paging - location specific - generally in decline
- SMS - not easily location specific - widely deployed
- CBS - location specific - not widely deployed
- MMS - not easily location specific - new service
- MBMS - not easily location specific - new service
- USSD - not easily location specific - designed for a specific purpose (e.g. mobile phone user preferences)
- E-mail - not easily location specific - widely deployed - feature rich.

- See ETSI TS 102 182 for more detail

Mobile Messaging Evolution

- SMS (1990) (3GPP TS-23.040 Point to point messaging Short Message Service)
  - Text Messages (160 Characters) but concatenation allowed for.
  - Binary Messages (140 Octets).
  - Widely supported.
- EMS (2001) (defined in 3GPP TS 23.040)

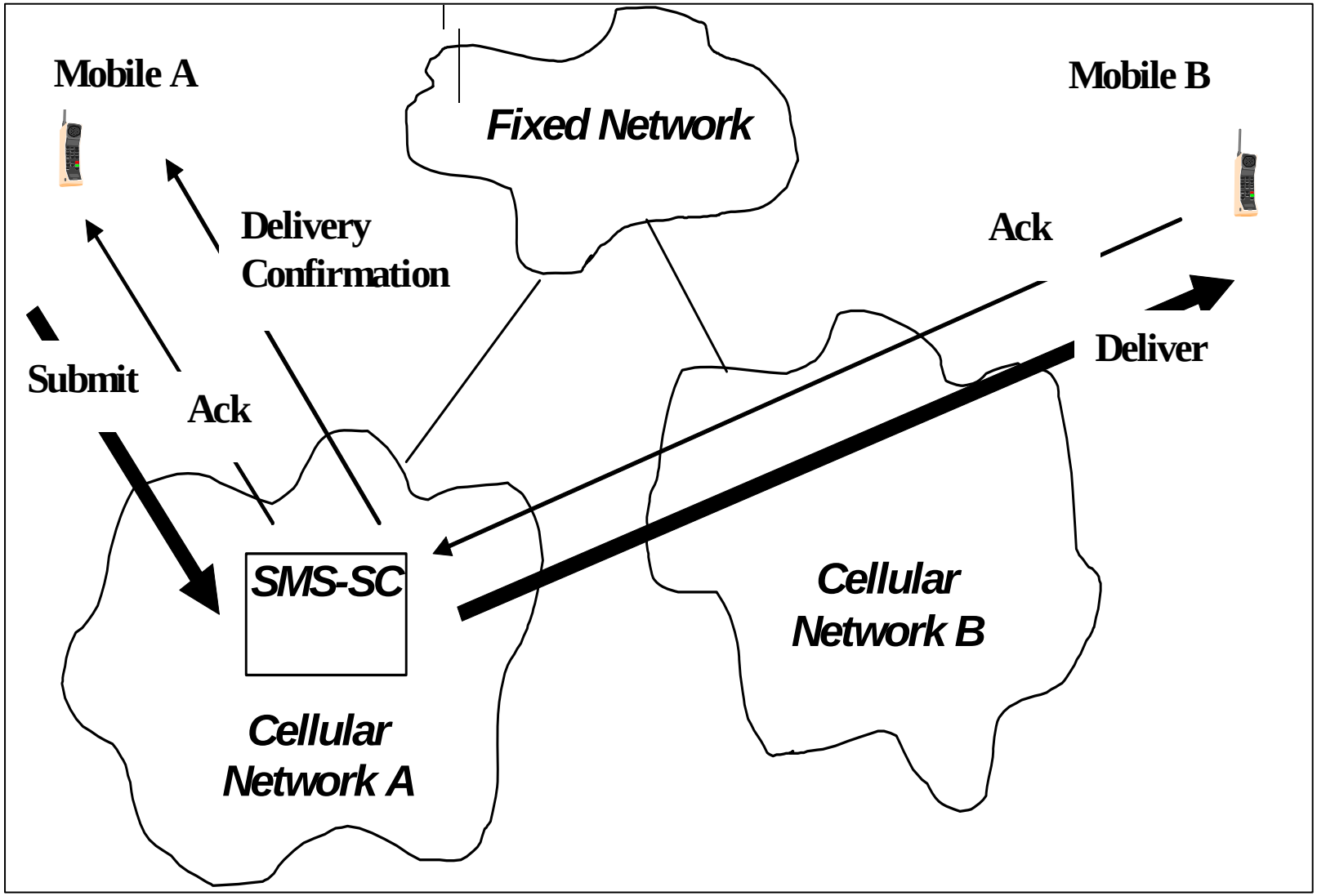
SMS plus the following

  - Vector Graphics (line drawing, simple animations), Polyphonics (orchestral sounds).
  - Not widely supported.
- CBS (1990) (3GPP TS 23.041 Point to Multipoint messaging Cell Broadcast Service)
  - Text messages up to 15 pages of 93 characters
  - Capable of broadcasting messages to all mobiles nationally or all mobiles in a specific geographic area down to a single cell.
  - Periodic retransmission of specific broadcast message between 2 seconds and 32 minutes.
  - Very little used - Power drain and MMI difficulties at the receiving mobile and difficult business case justification.
- MMS (2004) (3GPP TS 23.140 Multi Media Messaging Service)
  - Text ,Speech, Still Images, Video
  - Service in it's infancy.
- MBMS (2005) (3GPP TS 23.246 Multi-media Broadcasting / Multicast Service)
  - Text, audio, picture, video
  - Multicast requires subscription. Broadcast does not.
  - May have similar problems to CBS
  - Service in it's infancy

Short Message Service (SMS)

- Well tried and tested service – almost 15 years commercial operation.
- Store and Forward Service – virtually guarantees message delivery once message has been sent to Short Message Service Centre (SMS-SC).
- Not ideal for 2 way messaging applications where real time messaging is a criteria. Fixed network message termination can considerably improve real time performance.
- Reliable – but has characteristics that may give impression of unreliability. Receiving mobile turned off or in poor radio coverage is the main reason for message delivery delays heightening the perception of poor performance and unreliability.
- Billing mechanism well established.
- Supported in virtually every mobile network and by virtually every mobile.
- Virus free. No externally accessible executable environment necessary in the mobile.
- Will often succeed in poor radio conditions where voice calls do not.
- Biggest revenue earner next to speech.
- Cannot easily target mobiles in a specific area.
- Bulk SMS messaging for mobiles in a specific area is slow when the number of targeted mobiles is large.

SMS System Overview



SMS-SC Functionality

- Retry Schedules for messages
  - Operator and SMS-SC vendor specific.
  - Vary according to error condition.
  - Typical first retry 1 minute after initial attempt delivery failure.
- Alert
  - Triggers an SMS-SC into delivering a message if the receiving mobile becomes available having been unavailable.
  - Registration.
  - Location update.
  - Periodic location update timer in mobile.
- Delivery reports
  - Operator and SMS-SC vendor specific but not widely supported.
  - Must have been requested by mobile sending the message.
- Billing
  - Operator specific.
  - Delivery reports may be additionally charged for.
  - Difficult to charge recipient directly as no SMS call records are generally available in recipients network.
  - Sender can be charged by own network and may be charged by recipients network via own network.
- Fixed Network connectivity
  - Operator specific.

SMS Typical Performance – mobile to mobile

- Time between message sending from mobile to message received at recipients mobile – typically 6 to 8 seconds. Only about 1 to 2 seconds typically of this is attributed to message storage in the SMS-SC. See Note.
- Time between message sending from mobile to that mobile receiving delivery confirmation – typically 10 to 12 seconds. See Note.
- Typically 38% messages not delivered on first attempt – mainly due to receiving mobile out of coverage or turned off). See Note.
- Typically 98% messages actually delivered.
- High probability of Submission success and Delivery success because air occupancy is a few tens of milliseconds compared to several tens of seconds or more for speech.
- Message duplication can occur.

NOTE: For messages sent to a fixed network termination rather than a mobile, the delay figures above can be expected to be more than halved. Additionally, the probability of messages delivered on the first attempt can be expected to be 98%. Unlike the mobile to mobile case, the 'Message Sent' indication (Ack to the Submit) at the sending mobile phone can be taken to mean with a high degree of confidence that the message actually reached its fixed network destination.

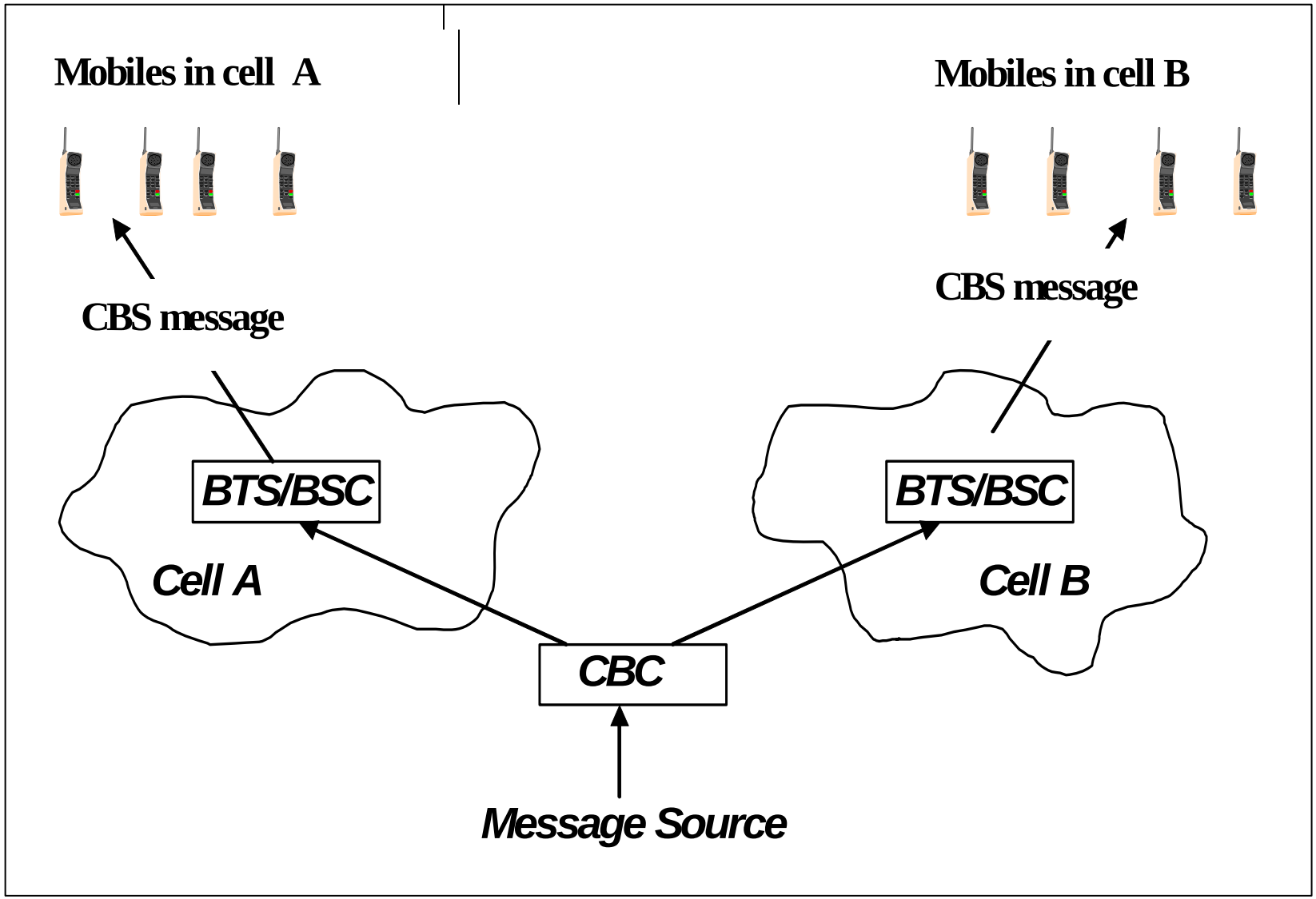
SMS Security/Authentication

- Messages are encoded according to the same encryption algorithm that is used for setting up and controlling a mobile call.
- The Originating address cannot be easily spoofed unless there are 2 mobiles that have been allocated the number or there is poorly policed internet access to an SMS-SC.
- Tapping into the radio path is possible but requires sophisticated equipment and considerable technical skills.
- Where security is an issue then end to end encryption must be applied.
- Tracing source of Spam / unwanted messages is time consuming and costly.
- Message could be authenticated by the recipient examining the Originating address.

Cell Broadcast Service (CBS)

- Very few services commercially operable.
- Virtually guarantees message delivery once message has been sent to the Cell Broadcast Centre (CBC).
- CBS messages are held in the CBC for a pre-defined period of time and may be deleted or updated.
- CBS messages may be sent to all mobiles in a single cell, a group of cells or nationwide.
- There is no acknowledgement mechanism from mobile phones to the mobile network.
- Receipt of CBS messages by the mobile relies on the user having enabled CBS on the mobile phone.
- Reliable – messages normally transmitted repeatedly to mobiles for a period of time.
- Complex commercial and billing issues. Business case justification difficult.
- CBS Capability inherent in many mobile networks infrastructure but not enabled.
- Virus free. No externally accessible executable environment necessary in the mobile.
- Will often succeed in poor radio conditions where voice calls do not.
- MMI on most mobile phones is not particularly user friendly and largely un-developed.
- Power consumption concerns by mobile phone vendors - once receipt of CBS is enabled.

CBS System Overview



CBS element Functions

- Message Source (usually outside network operators domain)
  - Content
  - Geographical area
  - Desired Repeat time.
  - Desired Validity period
  - Message identifier
- CBC (Usually inside network operators domain)
  - Stores CBS message until updated or deleted by Message Source
  - Identifies which cells relate to geographic area desired by message source
  - Downloads CBS message once to appropriate BSC with Message ID

  NOTE: Interface to Message source is CBC vendor specific and outside the scope of 3GPP specifications.
- BSC/BTS (co-located with a particular cell)
  - Holds CBS message until deleted or updated by CBC
  - Re-transmits CBS message at a period defined by CBC
- Mobile Phone
  - Requires CBS to be enabled on the mobile phone
  - Requires the particular Message ID to be selected in order to display a particular CBS message
  - Display of CBS message and MMI is mobile phone vendor specific

  NOTE. The following are essential.
  - Network availability.
  - Mobile registered.
  - Good radio coverage.

CBS Typical Performance

- Periodic retransmission from the BTS of specific broadcast message is between 2 seconds and 32 minutes.
  - The fastest periodic transmission period will degrade the more CBS messages require to be transmitted per BSC/BTS.
  - Network operators may have to degrade the ‘periods’ in order to safeguard against BSC/BTS overload.
  - For broadcast of national emergencies it may be necessary for a network operator to suspend broadcast of all other CBS messages in order to meet delivery criteria.

CBS Security / Authentication

- Most network operators do not permit 3rd parties to access the core mobile network protocol (CCITT No. 7 MAP) and so the risk of downloading false messages to the BTS/BSC is low. However, some network operators do allow 3rd party access to CCITT No. 7 MAP.
- The CBC is normally within a network operators domain and should police messages sent to it from a Message Source. However, there is no guarantee that this is the case for all network operators.
- The Message Source is normally outside the Network operators domain and there may be many Message Sources for various applications. Viz. weather, road traffic, advertising, national emergency messages.
- End to end encryption is complex and would require management in the mobile phone
- Tapping into the radio path is possible but requires sophisticated equipment and considerable technical skills.
- Authentication of National Emergency messages is a complex issue and there is no inherent aspect of CBS 3GPP specifications that addresses authentication.

CBS Business Cases

- All mobiles capable of receiving CBS messages will do so once enabled by the subscriber but with no opportunity for the information provided to be charged to the subscriber for the information received. CBS is a *Broadcast* service.
- Revenue can however be obtained in the following ways
  - Teasers (get recipient to make a telephone call for further information)
  - Advertising

Summary

- There is not one mobile technology that would satisfy all the service and performance expectations.
- Funding is a complex issue
  - Utilising a currently available commercially viable service to carry emergency messages can do so at little or no additional cost – as is the case for emergency speech telephony calls.
  - Developing a solution for the specific purpose of broadcasting emergency messages is unlikely to progress.
- Perhaps a more pragmatic approach may be necessary
  - Alerting by audible siren.
  - Different siren sounds could indicate different emergencies but would the public remember what each sound meant.
  - Once Alerted - provide further information by a combination of other currently available commercially viable means
    - Access a web site via email
    - Radio / TV
    - Access an information site via SMS

Standards for Business

End of Presentation