Cell Broadcast Technology for Public Warning

Synthesis of a Request for Information by the UNDP R3I

R3I
Regional Risk Reduction Initiative

UNDP
Empowered lives. Resilient nations.

This project is financed by the EU and implemented by UNDP

Citation: UNDP (2012) Cell Broadcast Technology for Public Warning: Synthesis of a Request for Information by the UNDP R3I. United Nations Development Programme, Barbados and the OECS

Author: Arthur Botterell
Editing: Danielle Evanson
Design: GreenLeaf Design Inc., Barbados

This resource has been possible thanks to the support of the European Union under the Regional Risk Reduction Initiative (R3I), which was implemented by UNDP Barbados and the OECS.

Cell Broadcast Technology for Public Warning Synthesis of a Request for Information by the UNDP R3I

Prepared by Art Botterell, Warning Systems Consultant

Contents

Glossary And Acronyms

2G	*Second generation wireless telephone technology, a family of technical standards deployed mostly in the years 1991-2001*
3G	*Third generation wireless telephone technology, a family of technical standards deployed in the period 2000 to the present.*
3GPP	*The "Third Generation Partnership Project", an international group of telecommunications associations initially dedicated to specifying the GSM standards and later extended to other standards including the fourth generation LTE standard.*
4G	*Fourth generation wireless telephone technology, generally deemed to include Mobile WiMAX (first deployed in 2006) and LTE (introduced in 2009). Note, however, that the first generation of LTE and also Mobile WiMAX systems do not meet the peak data rate requirements specified by the International Telecommunications Union in 2008, and therefore there is debate as to whether they should properly be termed "4G".*
Aggregator	*A digital facility for the central collection, storage and republication of messages. In a public warning system an Aggregator typically stores and makes available all current alerts, i.e. those alert messages that have not expired, been replaced by an update, or been cancelled. An Aggregator is frequently integrated with one or more Gateways (q.v.) to connect it to various input sources or message delivery systems, for example a Cell Broadcast Controller or Base Station Controller.*
AMICK	*Mr. Robert Amick*
Base Station Controller (BSC)	*The component of a cellular telephone system that manages the function of the actual cellular transmission stations ("cell sites"). A single BSC may control dozens or even hundreds of cell sites. Note that the term BSC is defined as part of the GSM standards but often is used to refer to comparable devices in systems using other standards.*
BSC	*see "Base Station Controller"*
CAP	*see "Common Alerting Protocol"*
CB	*see "Cell Broadcast"*
CBC	*see "Cell Broadcast Centre"*
Cell Broadcast (CB)	*A mobile technology for simultaneous delivery of messages to multiple users in a specified area without requiring duplicate transmissions to each recipient. Cell Broadcast was first supported in the ETSI GSM standard, but has been extended to UMTS networks, and comparable capabilities on other systems are often included in the use of the term.*
Cell Broadcast Centre (CBC)	*A digital facility for interfacing messages to one or more wireless operators' Base Station Controllers (BSCs) for transmission to mobile subscribers using Cell Broadcast. A CBC may provide various services, including customised interfaces to BSCs of different models, routing of messages to selected BSCs for geographic targeting, and message and alarm logging and exception handling.*
CELLCAST	*CellCast LLC*
CMAS	*see "Commercial Mobile Alerting Service"*
Commercial Mobile Alerting Service (CMAS)	*A public warning system under development in the United States of America that utilises Cell Broadcasting.*
Common Alerting Protocol(CAP)	*An international data standard for the exchange of public warnings and other event-driven notifications. The primary purpose of CAP is to make it easier to coordinate the operation of multiple public warning systems in order to increase their effectiveness and efficiency. Also known as International Telecommunications Union recommendation x.1303.*
CONICT	*Conict Consultants B.V.*

European Telecommunications Standards Institute (ETSI) — *A non-profit standards organisation that publishes standards, technical specifications, guides and other deliverables for Information and Communication Technologies (ICT) in Europe, which standards frequently have global impact.*

ETSI — *see "European Telecommunications Standards Institute"*

Gateway — *A digital facility for filtering and forwarding digital messages. In a Cell Broadcast alerting system a Gateway may provide a number of services including message authentication, content verification and format conversion. A Gateway frequently is a component of an Aggregator or a Cell Broadcast Centre.*

Global System for Mobile Communications (GSM) — *Originally "Groupe Spécial Mobile". A set of standards for "2G" wireless telephone service developed by ETSI and first deployed in 1991. GSM has been enhanced to "3G" levels by the deployment of UMTS (q.v.) and is expected to migrate to "4G" LTE standards in coming years.*

GSM — *see "Global System for Mobile Communications"*

Internet Protocols (IP) — *A suite of technical standards for wired and wireless data communication that form the basis of the Internet. Note that the "Internet Protocol" (singular) is just one of a number of standards making up the IP suite; it sometimes is necessary to clarify whether the term IP is being used to refer to that single protocol or the entire suite, although that often can be inferred from the context.*

IP — *see "Internet Protocols"*

LTE — *see "Long Term Evolution"*

Long Term Evolution (LTE) — *A wireless high-speed data communication standard first deployed in 2009. LTE is widely anticipated to become the first truly global mobile phone standard, although differences in radio frequency assignments in different countries may limit interoperability in some cases. LTE is generally regarded as a "4G" system.*

Message Identifier (MI) — *A four-digit number attached to each cell broadcast message, used to separate messages into "channels" addressed to different purposes or audiences.*

MI — *see "Message identifier"*

NCC — *National Crisis Centre*

OCTs — *see "Overseas countries and territories"*

Overseas countries and territories (OCTs) — *A term used to describe the status of colonies or dependencies of European countries*

R3I — *see "Regional Risk Reduction Initiative"*

Regional Risk Reduction Initiative (R3I) — *A project designed to strengthen the resilience of English and Dutch OCTs in the Caribbean to various natural and climate change impacts. Funded by the European Commission and implemented by UNDP Barbados and the OECS, the R3I involves improvements in hazard mapping and vulnerability assessment, response and recovery, comprehensive disaster risk management, cooperation and coordination among the OCTs, and a pilot public warning system deployment.*

Request for Information (RFI) — *A business process for seeking written information about a particular topic from experts, vendors and other sources. An RFI is sometimes a direct precursor to a request for tender or other procurement, but it may also be for purely informational purposes.*

RFI — *see "Request for Information"*

Service Level Agreement (SLA) — *A contractual agreement formally defining requirements for specific levels of technical performance. An SLA may also address responsibilities, priorities, guarantees, warrantees and penalties for non-compliance.*

III

SLA	*see "Service Level Agreement"*
UMTS	*see "Universal Mobile Telecommunications System"*
UNDP	*see "United Nations Development Programme"*
Universal Mobile Telecommunications System (UMTS)	*A "3G" mobile cellular technology developed by the 3GPP and based on the earlier GSM standard. First deployed in 2002, UMTS has since been upgraded for greater data speed, leading to it sometimes being described as "3.5G." In coming years UMTS is expected to be upgraded further as LTE (q.v.)*
United Nations Development Programme (UNDP)	*The global development network of the United Nations, connecting countries to knowledge, experience and resources to help people build a better life.*
WiMAX	*"Worldwide Interoperability for Microwave Access," a technical standard for high-speed wireless data communication over wide areas (up to 50km radius). WiMAX service to mobile phones ("mobile WiMAX") has been marketed as a "4G" wireless telephone system, although recently some vendors have shifted their focus toward the LTE standard instead.*

Introduction

"Cell broadcast" (CB) is a technique for transmitting data messages simultaneously to all wireless devices connected to one or more cellular wireless system transmitters ("cell sites"). CB has been used in a number of recent public warning projects worldwide, and is widely accepted as being more efficient and flexible than previous alerting mechanisms based on individual audio messages or Short Message Service (SMS) texts. Nations currently known to be using CB for public warning include the Netherlands, Israel, Chile, Japan and the United States.

The Regional Risk Reduction Initiative

Like the other small island developing states (SIDS) in the region, the English and Dutch overseas countries and territories (OCTs) in the WCR are highly vulnerable to various natural hazards and climate change impacts, and have fragile ecosystems. Settlements are often concentrated in low-lying coastal areas and other hazard-prone locations. The R3I is a 4-year project (2009-2012) funded by the European Commission (€4.932m) with the objective of developing the local capacities for disaster risk management of the beneficiary territories, namely Anguilla, Aruba, Bonaire, British Virgin Islands, Cayman Islands, Curaçao, Montserrat, Saba, Sint Eustatius, Sint Maarten, and Turks and Caicos Islands by:

- Increasing capacity in hazard mapping and associated vulnerability assessments, to further be incorporated into spatial information systems to inform planning and development processes
- Developing a regional Early Warning Systems (EWS) pilot for the OCTs, based on the International Telecommunication Union (ITU) automated alert protocol for warnings
- Building capacities in response, rescue and recovery through the use of risk assessment and mitigation practice in order to shorten recovery periods
- Strengthening local disaster management structures and capacities in terms of tools and best practices to support comprehensive disaster risk management schemes
- Enhancing cooperation and coordination between the OCTs, with documentation and dissemination of best practices

Indeed, the R3I project, by emphasising intra-regional learning and sharing of tools, knowledge and best practices has enhanced the territories' individual and collective capacities to predict and prepare for disasters, thus improving resilience and reducing risk and subsequent loss.

During 2011 and 2012, the UNDP sub-regional office for Barbados and the Organisation of Eastern Caribbean States (OECS) commissioned the REMPEITC to carry out OPRC workshops under the framework of the R3I.

The aim of this resource is to share technical perspectives on the capabilities and feasibility of implementation of an emerging technology in the region as various countries expand their EWS infrastructure to better serve their populations in the context of disaster risk management. This is particularly in light of the experiences of Anguilla, Aruba, Montserrat, and Sint Maarten in particular as they have strengthened/adopted the Common Alerting Protocol (CAP) structure for EWS.

The Request for Information

On 2 February 2012 the United Nations Development Programme office in Barbados published a Request for Information (RFI) regarding cell broadcast technology for public warning. This request, identified as RFI120217, was issued as part of a programme of public warning capability development in the British and Dutch overseas countries and territories (OCTs) in the Caribbean region as part of the Regional Risk Reduction Initiative (R3I).

The RFI requested expert advice on sixteen specific topics regarding CB implementation for public warning. The RFI was published by UNDP and publicised through emergency management and telecommunications organisations and online fora. Responses were received from:

Mr. Robert Amick, former Communications Director of the Department of Public Safety, University of Colorado, Boulder, Colorado, USA ("AMICK");

Mr. Tom Muggerud, UMS AS, a Norwegian firm offering a public alerting system they propose as an alternative to cell broadcast technology ("UMS");

Mr. Peter Sanders, one2many FC-LLZ, a Netherlands-based provider of Cell Broadcast alerting and advertising systems ("ONE2MANY");

Mr. Willy Steenbakkers, National Crisis Center, Ministry of Security and Justice, Kingdom of the Netherlands ("NCC");

Mr. John Tacken, Managing Director, Conict Consultants B.V., a project management firm involved in Cell Broadcast implementation in the Netherlands ("CONICT");

Mr. W.M. van Setten, Director, SPMM consultancy, with participation from the Cell Broadcast Form and CEASA-INT ("SPMM"); and,

Mr. Mark Wood, Chief Technical Officer, CellCast LLC, London ("CELLCAST").

Each of these responses provided valuable inputs and insights. The submissions by CELLCAST and SPMM were particularly noteworthy for their responsiveness and detail.

Summary of Inputs Received

The following are the questions posed in the RFI and a summary of the information received:

1.What technical steps must be taken in order to implement cell-broadcast based public alerting?

The respondents agreed that implementing CB-based alerting requires the integration of official, commercial and personal resources and that this can be a relatively complex undertaking.

- Government must provide an alert origination mechanism that provides authentication of alert originators and provide a mutually acceptable message-forwarding interface to each of the participating wireless carriers.
- Carriers must implement CB functionality on their equipment; while this capability is widely available, in some cases the carriers may have to pay additional fees to their equipment and software providers to activate it. Carriers may seek financial reimbursement, appropriate-use policies and legal exemptions from liability in exchange for providing technical support for CB alerting.

> "…the business model for Cell Broadcast is not very rewarding, meaning that handset manufacturers are not very enthusiastic to implement on the smart phones per default the CB functions" (SPMM)

- Individual cell phone owners may need to reconfigure their existing phones manually in order to receive the alerts. Cell phone vendors may be recruited to assist individuals in doing so and to pre-programme new cell phones; they may seek reimbursement or other incentives for providing these services.

2.How can the current and forecast penetration of cell-broadcast capable handsets in a particular OCT be assessed?

Although the respondents were generally optimistic about the number of cell phones that might be served by CB alerting now and in the future, they were generally reluctant to venture specific numbers. Several factors were mentioned to explain this uncertainty:

- SPMM reported that "Cell Broadcast is supported on almost all 2G handsets (>95%)… however the user has to select themselves the activation of the handset… the increasingly popular smart phones using 3G will NOT display the Cell Broadcast messages… it is in general not supported by the handset."
- CELLCAST reported "Something like 80% of all mobile phones have a Cell Broadcast feature enabled on them. Contrary to common sense, the older phones have better support for CB than the newer ones. Some modern phones have no support for CB at all, while others support only CMAS [the U.S. implementation] but not native CB."
- CONICT reported that in a survey in the Netherlands they found 58% of the handsets on the market were "technically capable" of receiving CB alerts. The date of this survey was not specified.

The distinction between the CMAS and "native CB" implementation, according to CELLCAST, has to do with an inconsistency regarding the "message identifiers" (aka "addresses," "channels," or "topics") used for alerting. Cell broadcast allows messages to be differentiated by a four-digit numeric "MI". However, CELLCAST reports that "Many terminals including Ericsson and Nokia allow the user to select manually only channels with three digits, 0-999." CELLCAST goes on to explain that the CMAS implementation uses MIs in the range 4370-4381, which cannot be manually programmed on some phones, whereas the European Telecommunications Standards Institute (ETSI) recommendation as implemented in the Netherlands uses MIs in the range 500-599 and 900-999.

CELLCAST adds, "Fortunately there is no problem at all in transmitting the message to both addresses at the same time."

SPMM notes other limitations, such as lack of CB support on popular iPhone and Android handsets, and comments that "the business model for Cell Broadcast is not very rewarding, meaning that handset manufacturers are not very enthusiastic to implement on the smart phones per default the CB functions."

3.What alert delivery formats (text, audio, images, etc.) are feasible using cell-broadcast technology?

The default format for CB, based on the limits of GSM systems, is a 90-character (using 7-bit characters) block. Although typically this is text, it could be binary data, and multiple blocks might conceivably be chained together into longer messages; such functionality would require additional software to be installed on handsets. On newer systems larger blocks of text and/or data can be broadcast.

SPMM also described the process of automatically generating such a brief text message from a Common Alerting Protocol (CAP) input alert, as is being done in the U.S. CMAS implementation.

4.What firms, organisations and agencies must be involved in a successful cell-broadcast alert system deployment?

As noted above, the three essential participants are government, the various cellular service providers and the public. However, the provision and operation of the government gateway to the cellular carriers, sometimes called the Cell Broadcast Centre (CBC) may sometimes be outsourced to an additional commercial entity.

Likewise, individual customer support will be required from the vendors of cellular handsets to the public who, depending on local market arrangements, may or may not be directly controlled by the carriers.

Public education activities required:
- General public education and expectation management regarding the scope and capability of CB alerting, placed within a larger system that coordinates multiple means of alert delivery
- Specific education of handset owners as to the steps required to programme their handsets to receive alerts

5.What public education activities are required in the course of a cell-broadcast alert system deployment?

Two general topics were identified:

1. General public education and expectation management regarding the scope and capability of CB alerting, which most of the respondents recommend should be placed within a larger system that coordinates multiple means of alert delivery; and,
2. Specific education of handset owners as to the steps required to programme their existing handsets (and any future handsets that are not provided pre-programmed) to receive alerts.

Several respondents commented on the importance of regular system tests, both for general public education and as occasions for individuals to verify their phones' programming.

CELLCAST added that, "The fact that Cell Broadcast is 'passive' and not 'tracking' users must be trumpeted very loudly. For many people, the prospect that the government is tracking them is a disincentive to participate."

6.What are the key issues which must be negotiated with wireless carriers to implement and maintain a cell-broadcast alert system?

Respondents (particularly CELLCAST and ONE2MANY) mentioned the following:

- A formal Service Level Agreement (SLA) with each carrier committing to provide CB alert transmission at a specified level of technical performance (reliability, speed, etc.), including a requirement that each carrier establish SLAs with its vendors and contractors as required to meet its own service-level requirements;
- Priority for alerts over other CB messages such as advertising;
- A forward-looking agreement to support CB alerting on all existing networks (2G, 3G, etc.) and future technology platforms (e.g. Long Term Evolution "LTE");
- A commitment to sell and support handsets and other mobile devices that support CB alerting;
- Limitation on the carriers' legal liability related to CB alerting;

7.What mechanisms are available for providing alerts in multiple languages using cell-broadcast?

Regarding the transmission of multi-lingual alerts, CELLCAST and SPMM both noted that existing Third Generation Partnership Group (3GPP) standards for 3G services specify a Data Coding Scheme (DCS) that permits transmitting a message in multiple languages. message."

"the distributing network will not be willing to accept any liability for the contents of a message, so very likely they will insist that the originator sends the message in a multi-language format at point of origination. This will prevent any liability for misunderstandings due to mistranslation or omission of a message." (CELLCAST)

However, SPMM said, “It is believed that NOT ALL Mobile Stations, the mobile telephone, support a language filter, although most of the leading Mobile Station – handset manufacturers have implemented this in a proper way.” SPMM also reported that “most of the handsets in operation… have selected ‘all languages on’. When this is the case the language filter is not in active operation.”

CELLCAST noted that GSM terminals can host fonts such as Chinese or Arabic, but not all fonts, and further, that font encodings which require more than seven bits per character (i.e. fonts that have more than 128 characters) will be able to transmit only half as many characters per message.

Operationally, CELLCAST observed that “the distributing network will not be willing to accept any liability for the contents of a message, so very likely they will insist that the originator sends the message in a multi-language format at point of origination. This will prevent any liability for misunderstandings due to mistranslation or omission of a message.”

8.What mechanisms are available for providing alerts to people who are deaf or hearing-impaired, and people who are blind or vision-impaired?

Respondents noted that many deaf or hearing-impaired individuals already have lights or vibrators attached to their mobile devices, and that many blind or vision-impaired persons use text-to-speech conversion software for accommodation.

SPMM noted that a special alerting cadence can be applied to vibration, lights and tones to signal special alerts. This method is used in the U.S. CMAS system.

9.Other than secure provision of the same input, e.g. a Common Alerting Protocol (CAP) message, to all carriers, are there any other special considerations, technical or procedural, which should be taken into account when planning cell-broadcast-based alerting in OCTs served by multiple wireless providers?

Respondents cited the following:

- Individual variations in the way alerts are identified in the distribution system. CELLCAST offered as an example the use of MIs in 2G and 3G CB vs. Internet Protocol (IP) multicast addresses in future systems.
- Geographic targeting of alert delivery. SPMM noted, “Governments want to be able to send out an alert as small as only one cell.” The reviewer adds from experience that in some cases even more precise targeting of an alert may be desired.
- Methods for verifying that alerts were successfully transmitted.
- “Heartbeat” mechanisms for verifying availability by detecting failures in the links between originators and carriers.
- Time synchronisation among all components of the system.
- Integration with other public alerting systems.
- Integration with official notification systems to ensure that appropriate officials are notified as soon as an alert is issued, even if they are not in the alert service area.

This question also elicited comments regarding the role of the Common Alerting Protocol (CAP) in CB alerting generally. ONE2MANY remarked that, “The CAP protocol is not a protocol that can be implemented directly for CB based alerting,” and stresses the role of the gateway/CBC in converting from CAP to the specific interfaces required by the cellular carriers.

Many deaf or hearing-impaired individuals already have lights or vibrators attached to their mobile devices, and that many blind or vision-impaired persons use text-to-speech conversion software for accommodation

SPMM suggested, “The CAP standard is quite a new standard and could be changed in some details.” CELLCAST noted that, “CAP does not in its present form have a field for defining the requested MI code.” The reviewer notes that this last item would be an appropriate use of the existing CAP “parameter” element.

Cellular network service areas do not necessarily coincide with political boundaries, nor do hazards respect administrative or sovereign bounds, and that this creates requirements both for careful engineering of alert distribution systems and for a degree of reciprocity regarding urgent warnings in adjacent jurisdictions.

10.What are the various costs involved in deploying cell-broadcast-based alerting, both initial and recurring, and how may they be estimated?

- In some cases, additional licensing fees to network technology providers for activation of CB features.
- Procurement or development of the government gateway/CBC and its installation, testing and maintenance.
- Service fees to the carriers.
- Costs of identifying and training alert originators and of issuing, reviewing, maintaining and revoking access credentials (passwords, digital certificates, etc.)
- Costs of ongoing governance and auditing of the overall system.

11.Are there any policy or procedural considerations that are unique to cell broadcast-based alerting?

ONE2MANY suggested a requirement for periodic repetition of CB alerts for as long as the alert is valid, to serve handsets that have just been turned on or just entered the alert area.

CELLCAST pointed out that cellular network service areas do not necessarily coincide with political boundaries, nor do hazards respect administrative or sovereign bounds, and that this creates requirements both for careful engineering of alert distribution systems and for a degree of reciprocity regarding urgent warnings in adjacent jurisdictions.

12. For localised events, how precisely can the distribution of alerts over cell broadcast be tailored to fit originator-specified geospatial boundaries, which may be a priori administrative boundaries or ad hoc bounds developed at the time of an event reflecting a particular set of circumstances (e.g. a “plume model” for a hazardous material release)?

The respondents agreed that the current minimum resolution of CB alerting is defined by the coverage of a single cell site, which may be quite irregular in shape and vary in range from less than 1km in dense areas to 30km. or more in rural areas. The selection of the appropriate cells to transmit a targeted message can be achieved at the gateway/CBC or else within each carrier’s own system; the essential requirement is an up-to-date computerised map of the current configuration of each carrier’s cell transmitters and antennas.

CELLCAST observed that there are potential future methods for providing even more precise targeting of alerts, but those are not feasible in a 90-character message scheme.

13.In applications for notification of specific personnel, how can cell broadcast be used to notify a particular pre-identified group of individuals (e.g. public safety officers) regardless of their location within the service area?

Broadcast communication to either pre-identified or ad hoc groups can be achieved by designating a special MI for such messages and ensuring that all members of the group have CB capable handsets. CELLCAST noted that this scheme is only relatively private and not necessarily secure since it could be monitored by anyone who knows the correct MI. Additional encoding or encryption would be possible, but would require additional software on the handsets.

14.How can cell-broadcast technology support individual acknowledgement of receipt of alerts and the collection and review of such acknowledgements at one or more operations centres?

Cell Broadcast does not offer an intrinsic capability for returning individual acknowledgements or receipt. Several respondents point out that in many public warning applications the number of acknowledgement messages required could itself congest the cellular networks.

CELLCAST suggested that for limited groups a CB alerts could include a target URL for an "out of band" manual acknowledgement using IP connectivity, which could even be automated using additional software on the handsets.

SPMM mentioned that, while it is not feasible to report an acknowledgement from every receiving handset, most cell sites have a dedicated monitoring device which could, in principle, verify transmission by that individual cell.

15. What changes, if any, can be expected in cell-broadcast technology as new wireless standards such as LTE are adopted in future years?

> Broadcast communication to either pre-identified or ad hoc groups can be achieved by designating a special MI for such messages and ensuring that all members of the group have CB capable handsets

The respondents agreed that all foreseeable mobile wireless technologies will have at least as much capability as existing CB systems.

SPMM cautioned "The official standards for 3G and LTE have specified the Cell Broadcast function, but the commercial demand and drive for it is quite low… The network technology is not the limiting factor, it is whether handset manufacturers will build in the Cell Broadcast receiving function in the new smart phones in the coming years and this is very much market driven."

Several respondents note that the scale of CMAS in the U.S. market may increase handset support, although there may be some interoperability issues, particularly as regards the MI assignments. CELLCAST and SPMM both identified this as an active area of discussion in the CB community.

Summary Observations and Recommendations

Today's cellular telephone systems are among the most complex and pervasive systems ever devised by humankind. Through careful design and engineering they have been made to appear as relatively simple and consistent global utilities. Considered closely, though, they prove to be highly evolved artefacts of advanced technology, commercial enterprise, government jurisdiction, and social and community relationships.

Implementing public warning over cell broadcast involves subtle but manageable technical arrangements. More challenging, perhaps, are the arrangements between governments and private entities, among private entities and among governments, required in order to realise the promise of that technology.

In light of this reality, a recommendation may be made that governments considering the deployment of cell broadcast for public warning should first verify that they have the legislative and regulatory authority and the fiscal resources to make and sustain the required operational, technical, administrative and contractual arrangements.

Many of the respondents to the RFI recommended that cell broadcast be implemented in concert with other warning delivery systems, both to maximise the technical reach and reliability of the integrated warning capability, and also to maximise the public response through reinforcement of the message over multiple media. AMICK noted the extensive body of social-science research into the social and psychological components of public response to warnings.

Based on that research a strong recommendation may be made that any nation, jurisdiction or region contemplating CB alerting should first develop an integrated warning management mechanism usable for all hazards.

The programme of warning system enhancements being provided through the R3I, which executed the Request for Information and commissioned this summary, is deploying tools by which authorities can use all available warning media in concert to alert the public to any urgent and severe hazard. Cell Broadcasting, as it is more widely adopted, will be a valuable addition to that larger framework.

About the Reviewer

Art Botterell is a consultant to the UNDP R3I public warning programme. He is the originator of the Common Alerting Protocol and a member of the U.S. government committee that designed its CMAS cell broadcast implementation. He has designed, implemented and operated a number of public warning and notification systems in the U.S., and served as an advisor to scientific and disaster management agencies in North America, Europe, Asia and Australia. He is a member of the staff of the Disaster Management Initiative at Carnegie Mellon University's Silicon Valley campus in California.

Annexes

Source References

AMICK	Mr. Robert Amick, former Communications Director of the Department of Public Safety, University of Colorado, Boulder, Colorado, USA
CELLCAST	CellCast LLC, London, England and St. Charles, Missouri, USA
CONICT	Conict Consultants B.V., Ultrecht, The Netherlands
NCC	National Crisis Centre, Ministry of Security and Justice, Kingdom of the Netherlands
ONE2MANY	one2many, Deventer, The Netherlands
SPMM SPMM	(Stichting Platform Mobile Messaging), Hoofddorp, The Netherlands
UMS	UMS AS, Oslo, Norway

Emergency telephone notification systems for natural hazards

3 February, 2012

Bob Amick, ENP, (ret.) Communications Director, DPS University of Colorado at Boulder
amick@spot.colorado.edu
rdagto@msn.com
970 274-6557

I might suggest you contact the emergency management coordinator at the University of Colorado at Boulder Department of Public Safety. I retired as DPS Communications Director in 2004. In about 1995 CU had installed two Whelen electronic voice and tone sirens on the central and east research campus respectively. Initially they were the only public address voice capable electronic warning sirens adjacent to the City of Boulder which surrounds the campus. Boulder Creek runs through the middle of the campus for both housing and academic buildings and poses a serious flash flood risk. Then the city/county director of Emergency Management persuaded the city to also install this type of siren to replace their old mechanical/air sirens and gradually all of them were upgraded. CU-Boulder has a resident/commuter student population of about 31,000, and Boulder is around 100,000.

In the meantime, we had a public relations campaign each spring as part of a flood awareness exercise to reach the campus and Boulder Community as to what the sirens were used for and tests were conducted once per month at 10 am from April through August. Newspaper articles announced the tests and addressed appropriate response (i.e. to tune to local radio and TV stations for more information, as no internet web warning venues were yet available). We actually did some surveys of campus and community members and found that they, first of all could seldom hear the sirens inside their homes, buildings/workplaces, and especially not at night when they were sleeping. Secondly, they didn't understand what the sirens meant and what action they should take in the event of a flash flood (Boulder has the highest flash flood risk of any community in Colorado).

So we set about to distribute brochures to residents and community members, added cable TV interrupt capability for TV stations, et al. The worst mistake that anyone can make is trying to associate different warning tones with a particular emergency or hazard. The old civil defense codes that associated a long continuous tone with a warning, and a warble tone with an attack etc., were never understood by the public and research showed that most had no idea what the different tones meant, nor what they should if they heard a given tone. Some emergency managers assume that people know what the tones mean and what they should do to respond, but research has proven that they simply do not. Public address messages are somewhat better if used in conjunction with siren tones, but even they are often not heard or misinterpreted and hence are not the best way of conveying an accurate and effective warning message.

Despite all this, most folks still were oblivious to the siren tests and found them annoying. We interviewed people walking in the flood path on trails and bikeways to see if they knew what the sirens meant during the testing, and most said no, and that they thought they were just testing whenever they were sounded. Most said they would not know what to do if the sirens announced a flash flood, but were interested in learning more. Most did not associate Boulder Creek with a high natural hazard risk and consequently were not concerned about walking along the bike path next to the creek or living in family housing buildings adjacent to the creek.

So we set about developing the first high speed rapid telephone fan-out warning system in conjunction with Intrado Communications who marketed a product that used the 9-1-1 emergency telephone subscriber database to selectively call wired phones in the "polygon" or geographic zone defined to be "in harm's way" from a flash flood or other natural or manmade hazard. This system was adopted by the local telephone service provider Qwest and was initiated by the Boulder Regional Communications Center, and/or our own campus public safety communications center dispatchers. We also controlled the siren activations by radio link. The system was adopted county wide as the first fan-out telephone warning system in Colorado and was often used for wildfire warnings very successfully.

With the advent of cell phones and ipads, less wired phones are being used, so it was necessary to adapt to a system that covered both wired and wireless phone technology. Wireless requires proactive subscription by the subscriber where wired phones are automatically included in the fan-out system if their phone is in the 9-1-1 database but all are wired and wireless phone subscribers encouraged to enter their information into an online database to be sure that the information is accurate and current. Some aspects of wired phones that have call blocking may interfere with delivery of emergent messages, so subscribers have to be informed by TV or radio to have their phone service provider disable their call blocking unless they can do it themselves by command from their own phone. This was learned by accident during a wildfire fan out notification where many folks with call blocking did not get the message and inquired why they were not warned.

Another issue is PBX systems (private business exchange) that many universities and businesses use, as do hotels, et al. Those numbers must also appear in the 9-1-1 database along with automatic number and location identification technology to allow the emergency notification system to identify the physical location of the phone by address and phone number to route warning messages to those phones identified as being in harm's way. Technology exists to adapt PBX systems for 9-1-1 ANI/ALI data base file storage and for routing of emergent messages. PBX systems can also choke on high volume delivery of warning messages as they may only have limited inbound trunks to serve thousands of phones. For example a university might have 15,000 wired phones but only 300 inbound trunks to receive inbound calls, so if a notification system is flooding the PBX with 2000 calls and only 300 trunk inbound lines are available, the system will busy out and call deliveries will be delayed. Cell systems may suffer similar overloading with the delivery of bulk and simultaneous warning messages to various cell towers serving a given area. So all this must be considered in the planning of such warning technology.

For wired phones, the 9-1-1 database has the most current and updated address information and includes non-published numbers that conventional directory files do not include so wired phone subscribers are more likely to be accurately notified if this database is part of the notification system. Some states limit access to this information so it may be necessary to get special authorization to use it for public safety warning technologies.

These warning systems must also be carefully controlled and policies set for only specific hazards warning categories. Natural and man-made hazards are of course legitimate uses, but some agencies have used them for non-emergent and non-critical information dissemination such as where to vote, municipal events, etc., which tends to cause the public to become jaded about the messages that are sent out and they may ignore an actual warning thinking it is just another informational blurb about something that is not a life safety issue. Use of the 9-1-1 database for such uses may be prohibited by law in some jurisdictions so policies should be in place to prohibit non-emergent use of the system.

Service providers of notification systems must be carefully evaluated for reliability and redundancy such that in event of a major systems failure, they have backup or failsafe technology in place and in different locations that can instantly assume the distribution of messages despite the loss of a primary system server in a given location. Testing of that redundancy in pre-emergent conditions must be conducted to verify robustness and reliability of the system.

After the system was installed and tested, and test call messages were sent out to subscribers in the affected areas, and then surveys were made to determine system efficacy and what the campus and surrounding community thought of the warning system combination. The surveys indicated that the telephone fan-out system was by far the most effective because it delivered a specific hazard warning message describing who the warning authority was (e.g. sheriff, fire chief, police chief, et al), what the specific threat or emergency was (e.g. flash flood, tornado, haz mat spill, etc.), projected time when it would arrive, what areas would be specifically affected, and what specific action that residents should take (e.g. evacuate, shelter in place, etc.). This was felt to be by far the most reliable and effective communications emergency warning modality by those surveyed.

Part of the problem is that of typical human behavior to emergency warnings. Dr. Dennis Mileti, (former) Director of the renowned Natural Hazards Center at the University of Colorado at Boulder was also a foremost authority on human behavioral response to emergency warning methodology and reviewed our plans and our message structure in terms of what worked best. He wrote the warning protocols for the Oak Ridge National Atomic laboratories. So we tailored our messages to meet the criteria he developed as a format, (and as described above) and found that residents responded favorably and appropriately to those message formats. The CU NHC research indicated that people tend to deny or question threats to their safety such as natural hazards and go through a verification process by asking others if they are aware of a threat, or looking at radio and TV to confirm, or actually going out to observe if a threat exists. In the case of flash floods and tornadoes this is often a fatal mistake as valuable time is wasted when it would be better spent evacuating or seeking a safe shelter and has resulted in loss of life and injury as a consequence of delay. That way, there is little need for them to confirm or compare the existence or accuracy of warnings, and they tend to react much more quickly and appropriately than if they were not convinced of the reality of the warning.

http://www.colorado.edu/hazards/

So the bottom line is to use a multifaceted media warning system that delivers the same message through a variety of media channels such as by radio/TV (EAS), wired phone, internet website/e-mail, social media/cell phones, et al. CU Boulder has such a system in place where subscribers are called on their cell phones, get text messages on their ipads/computers, and links to the website that describes the emergency, so the message is going out widely and through many different channels to optimally reach as many folks as possible as quickly as possible. Multi-lingual messages are also important and can be delivered to non-English speaking community members if they specify that they do not speak English, but they have to so indicate what language(s) they speak when they subscribe. Similar warning devices can be provided for disabled/hearing/vision impaired if it is specified at the time of subscription that the subscriber has a specific disability.

Do not rely on sirens as the only means of warning. They are probably the least effective of all the technologies, and often the most expensive with only a limited circumference of effectiveness. They have too many shortcomings and are often ineffective unless folks get specific and similar warning messages from the public address function, or understand that the tones mean to check their internet/e-mail, radio/TV and other media to determine if an actual threat exists. Also the sirens are often drowned out by noise from severe storms/wind and other environmental conditions. As noted above, sirens were never intended to be heard inside buildings or while residents are sleeping, so they really only work well for folks outside on foot. Other buildings or terrain can cause sound reverberation and echoes that may cancel out or distort the voice announcements in some areas, so there are lots of potential side issues with warning sirens and public address functions. Moreover, they often cannot be heard inside moving vehicles especially if windows are rolled up due to traffic noise and insulation of vehicles to outside noise.

Ongoing public education of the community is essential as people tend to forget, or are simply unaware of the risk, unless they experience actual natural hazard events often such as tornadoes. In Boulder there hasn't been a serious flash flood in over 100 years, yet it poses the greatest threat to loss of life and property of any hazard and presents the least amount of advanced warning despite flood detection systems, other than perhaps a tornado which is far less likely to occur, or be of any major consequence in a mountainous area. With international students such as those from the Middle East, the concept of a flash flood is completely unfamiliar or plausible to them so it takes extra education with videos and media to illustrate how they are vulnerable to those risks.

The City of Boulder and the University of Colorado at Boulder cooperated to make a video called flood watch that illustrates the risks of flash foods, and also did one on 9-1-1 systems and the fan-out calling system to educate the public on how these systems work. You can view these online if you like as they are good training and public information tools for natural hazards such as flash floods and wildfires and also a good way to educate folks on proper use of 9-1-1.

http://www.bouldercolorado.gov/index.php

Use the drop down menu to select flood watch and Boulder 9-1-1 videos, then click on load. It takes Quick Time or similar media player to view.
Feel free to check with the CUDPS emergency management coordinator and/or the Boulder city/county office of emergency management for more details on warning system technology and applications.

http://www.colorado.edu/alerts/
http://boulderoem.com/index.php?option=com_content&view=article&id=60

Another valuable resource is the National Emergency Number Association [NENA] standards for fan-out emergency telephone notification systems that have included many of the technical and operational concerns and issues that must be addressed by such systems. I served on the committee that wrote those standards.

http://www.nena.org/resource/collection/ABEAA8F5-82F4-4531-AE4A-0AC5B2774E72/NENA_56-003_Standards_for_Emergency_Notification_Systems.pdf

UNDP RFI 120217
Cell Broadcast Technology for Public Warning

Mark Wood, CellCast LLC, London, 14 Feb 2012.

1 What steps must be taken to implement CB based public alerting?

1. trust protocol
2. network functionality
3. CBC integration
4. gateway programming
5. front end preparation
6. training of staff
7. education of the public

1.1 Trust protocol

Public warning is as much a political issue as it is a technical issue, so the technology must fit the politics or it will never fly.

Cell Broadcast based Public Warning needs a new form of cooperation that has not been seen before. It is impossible to transmit a Cell Broadcast message without the explicit cooperation of the distribution network, because Cell Broadcast messages are transmitted from the Base Station Controller (BSC) via a Cell Broadcast Center (CBC), and not through normal access via the MSC that the public may have.

The networks will have many terms and conditions before they will be willing to participate, some of them will be technical and some of them legal. For example they may limit the size of any text message transmission that they are willing to send, and they may insist on indemnity from any liability arising from participating. There may also be further conditions regarding compensation to the network for the use of their resources, or stipulations as to how Authentication and Authorisation of originators must be performed.

All of these matters may be collectively known as the 'Trust Protocol', which may be a collection of Memoranda of Understanding and other instruments designed to define the terms of the relationship.

The terms of participation may have an impact on the technology applied, so it is good to have a clear idea of this matter before the technology is designed.

1.2 Network functionality

Not all system technologies support a point to multipoint broadcast multicast bearer service. Of those that do, there are differences in the way the technology is implemented in the system.

Generally, Cell Broadcast is implemented by re-arranging the logical control sub-channel structure on the broadcast timeslot of the broadcast carrier of the cell.

No hardware changes are needed, but the feature is resident in the base station software and needs Initiating.

Once the feature is initiated, it will automatically re organise the Cell resources to make room for the Cell Broadcast channel.

Cell Broadcast is often bundled into the cost for the network and enabled by default, because the popular 'Cell Information' feature works by cell broadcast channel 50. However if it is not enabled, the network needs to enter a product key into the operating system in order to initiate the feature.

In some cases the cost of this has been unbundled and the network needs to contact the base station vendor to arrange for payment for the key. There is often times a procedure of benchmarking to follow to be sure that the additional feature has not degraded the performance of the network. Each network will have its own policy in this regard.

1.3 CBC integration

Though it is theoretically possible to administer Cell Broadcast directly from the BSC, in practice a Cell Broadcast Center is usually installed upstream of the BSC. This has many features including but not limited to;

- Keep translation tables so that the API can be used which is applicable to the specific model and make of the BSCs concerned. Some networks have more than one BSC vendor in their network, so the CBC needs to perform translation of requests. In the future, new system technologies may emerge with different API requirements, so the CBC makes the system future proof.
- Handle alarms and exceptions regarding such signalling.
- Since CB is a geo specific technology, the CBC needs to have a data base which reveals either the geographic location of the antennas, or the geographic coverage of the cells, depending on the model of the CBC. The CBC converts the WGS84 polygon from CAP into a fully qualified global address for the cells concerned and their applicable BSCs. It needs to do this for each frequency band and system technology separately.

The CBC vendor carries out integration not only of the signalling links, but also of automatic methods for updating the cell data files or coverage prediction files. Procedures for updates of these files on a regular and also exceptional basis are all part of the CBC integration procedure.
The CBC vendor takes care of this matter during integration process.

1.4 Gateway programming

The reason why we have a gate is so that we can close it (otherwise it is a hole). Since no one has total universal sovereignty, each originator has defined geographic jurisdiction over which this originator may send alert messages.
The purpose of the gateway is;

- To aggregate proposals for alert messages from multiple originators possibly using multiple origination systems.
- To authenticate the originators, the transmission methodology and the messages themselves so that only authentic originators may make proposals.
- To authorise senders on the basis of both Boolean logical parameters but also geographical parameters. For example the sender may have permission to send to a specific area of jurisdiction, but also additional permissions under mutual aid agreements with other jurisdictions in some circumstances. The polygon of any subsequent proposals that the originator makes are processed using polygons of jurisdiction for those originators before an authorisation is done. Many permutations of normal and exceptional processing are possible.

- To distribute the Authorised messages as 'Submissions' to multiple distribution networks, which may be cellular, IP systems, or other technologies such as RDS, broadcast or signage for example. Transformation of the message may be needed in order to meet the requirements of some of the participating networks. The logic can be arranged such that some participating networks can agree to accept a specific message on the basis of filtering parameters, while others may decline to do so.
- To provide a transparent platform on which all stakeholders can be fully informed of the process of gate keeping, involving comprehensive reports and alarms of any activity relevant to the stakeholder. The amount of offered traffic can be quantified for administrational or dispute resolution purposes.

1.5 Front end preparations

The Gateway needs certain information in order to meet the requirements set upon it by the stakeholders including the participating distribution networks.
Ideally a CAP formatted message should be sent to the gateway so that it can determine if the originator is Authentic and his message can be authorised. Specifically a 'Polygon' or other Geo-code is needed to specify the geographic scope of the proposal.

The gateway may decline any message which does not meet the requirements for authentication, so the front end device which the originator uses to create the messages, must be able to create from a user friendly GUI, a properly formatted proposal that the gateway can process. If the originator is an automatic device such as a water depth gauge, then it also must generate properly formatted proposals or the message will be declined. Accordingly a front end system which is user friendly yet capable of handling all the parameters needed for authentication, is needed. The originator is free to select a vendor of his choice in this matter, or he may have existing software of his preference, but measures must be taken to ensure gateway acceptance.

1.6 Training of staff

Recent years have seen great progress in the types of distribution methods available to reach the people. Alas emergency management experience and knowledge is still keeping up with the dizzying pace of progress. Therefore the originators need to be well trained on the use of their chosen front end system, and be conversant not only with the national or regional customs regarding the format of messages, but also of any limitations or recommendations regarding its presentation to the citizen in new formats.
The best way to understand all of this is to have regular exercise with the new technology. For example Cell Broadcast has channel (4381) for the use of originators so that they can practice their art without in any way involving the public.

1.7 Education of the public

The point and purpose of all of this effort is better public safety through reduction of vulnerability to hazards. The citizens need to be at least informed, and better still educated as to what emergency messages are and what they mean. Awareness before a disaster has been shown to be a huge force multiplier even greater than that provided by the technology itself.

In fact the exercise of reaching out to the public by the government can be a trust building process of its own merit.
Young people in particular are always excited to see their country being up to date with current technology, it give them pride in their country as well as giving them a good incentive to be fully involved in community activities to do with preparation.

2. Current and forecast penetration of CB capable handsets

This point is one of difference in opinion, and one in which the ETSI and CMAS systems have taken opposite views. To answer this question needs a word of explanation about the issues before I explain the answers.
Something like 80% of all mobile phones have a Cell Broadcast feature enabled on them. Contrary to common sense, the older phones have better support for CB than the newer ones. Some modern phones have no support for CB at all, while others support only CMAS but not native CB.
In its 'native' form, a user may enable Cell Broadcast in the three following ways.
First the user must 'enable' the CB service. In some cases the phone is sold with the CB by default OFF, and in some cases with it by default ON. In some cases, the phone has the feature on but the SIM card hides the user interface so that the user can't even see that the feature is there at all until the SIM card is changed.
When the feature is enabled, individual Message Identifiers (multicast addresses also known as Topics) must be enabled. A cell broadcast message begins with a 16 bit code which identified the 'Topic' (e.g. Weather, Traffic, Alerts), if the phone has not been commanded to intercept this code, it will ignore it and go back to sleep.

There are three ways that the phone can enable an MI

- The user can enable the number manually via the menu on the phone
- The user can select a topic by its text description on the index channel
- The network can command the phone to open a channel via an 'Over The Air activation' command (OTA). This is a special control message SMS sent to the phone giving the command to open a channel.

However some terminal vendors believed that Cell Broadcast was of little interest, so some of them removed or denigrated the feature. When the use of Cell Broadcast became mandatory due to its selection for EU-ALERT and CMAS, they then started to sell phones in which native cell broadcast was still hidden, but the CMAS alert channels could be enabled by special software loaded on the phone for this sole purpose. This is frequently the case in the USA.

In the USA, in future all phones sold will have to support CMAS, or the vendor at point of sale must tell the customer that it does not support CMAS.

But many mobile networks take a different view and see Cell Broadcast as a powerful new tool for delivering certain types of service where mass scale distribution is needed, so in many other countries the Cell Broadcast service is sold by default ON, and is fully functional to the user.
A further difference as to if a phone can be seen to be compliant is the matter of the special alert tone. In the USA, the CMAS system considers that a mobile must make a special alert tone (reminiscent of the EAS tones) when an alert message is received. The EU-ALERT system also has this as a future requirement, but allows that legacy phones already in circulation may produce only the normal tone, at least for now, when receiving an alert. In future all phones sold will have the special alert tone feature.

By far the most controversial matter is to do with the address space used for cell broadcast alerts. Many terminals including Ericsson and Nokia allow the user to select manually only channels with three digits, 0-999. So if the member state wants the most possible number of people to participate, and there is a large population of present model phones out there, then obviously choosing and address space between 0-999 if preferable.

However the CMAS standard decided not to support the present cohort of phones, and reasoning that the new phones would have the new software to enable them, chose 4370 - 4381 as the start of the address space. This means that many people won't be able to receive CMAS messages until they buy a new phone.

In a developed country most people buy a new phone every two years, so this is not a big problem, but in poor developing countries where the population is at much greater risk, older 2nd generation phones will be in common use for many years to come.

Therefore the EU-ALERT standard promulgated by ETSI requires that MIs below 999 be used (in addition to 4370), and in fact in the Netherlands MI 919 is used in the 'legacy' blocks 500-599 and 900-999.
Fortunately there is no problem at all in transmitting the message in both addresses at the same time, thus being compliant with both CMAS and ETSI at the same time. However the GSMA have yet to provide a framework for channel harmonisation in this address block, preferring their members to do so and then register their choice with them. Presently member states must make their own choice in the legacy address block, though rapid progress is being made now so this may soon change.

3. What delivery formats are possible with Cell Broadcast?

Cell Broadcast was originally conceived about the same time as SMS was conceived, and by the same team of people.
In 2nd generation GSM, cell broadcast can transmit 80 bytes of data per 1.8 seconds, and up to 15 pages can be concatenated into a single message. In practice in GSM a seven bit code is used, so this amounts to 92 characters. However two characters can sometimes be used for language identification so a payload of 90 characters is agreed as the practical payload of a CB message of a single page. There are variations among terminals as to how multiple concatenations are handled, and since some of them to not handle concatenation well, for the present, CMAS has decided to limit to 90 characters of text. (The value is different for fonts which need two bytes, of course).
However in 3rd and 4th generation, a fixed timeslot system is not deployed, so in theory there is no limit to a broadcast size. Indeed it is an ambition to use 4g for such things as sports event broadcast in the future. There is now a broadcast/multicast channel associated with each cell which has theoretically megabytes of capacity. So in theory in the future far more interesting content can be provided than merely text. This may include images, voice messages, video or active script.

4. Which firms, organisation and agencies must be involved in CB?

Cell Broadcasting needs the involvement of several stakeholders who have not worked together in this way before. I would recommend that a Trust Protocol group or steering committee be formed as a round table platform for dialogue with the stakeholders so that matters can be agreed.

At the least, these stakeholders should be

- The participating network whose resources are being used and whose customers are being targeted.
- The originators of information who would like to distribute information to the public.

The participating networks may have many concerns and need certain reassurances both technical and legal before proceeding, and so these two stakeholders may decide to involve one or more other actors as part of their checks and balances agreement.

However there may be different criteria depending on the nature of the messages to be distributed. For example weather forecasts may be provided by an independent or even private entity, while orders to evacuate may have to come only from national authority such as police officers depending on local law, custom and tradition.

They may require that a government ministry guarantee indemnity for the participating network. That ministry may have their own conditions to add both the participating networks and also to the originators.

For example there may be requirements not to transmit messages to locations which are outside of the lawful jurisdiction of the originator, or there may be differences on who can say what, where, when and how.

In order to assure stakeholders that the agreements will be faithfully kept, the trust protocol group should install a Gateway unit, so that the agreements can be honoured automatically by a computer system. A Gatekeeper should be appointed to administer the admission control system of the gateway on behalf of the trust protocol group.

A vendor should be selected to provide a gateway capable of supporting the requirements of the trust protocols.

Parties may decide that given the importance of reliability for a public safety system, a contractor should be appointed to provide the technical platform for the system, e.g. hosting of the computers in robustly secured locations, and multiple robust forms of transmission to connect the stakeholders together, bearing in mind that they will be doing so during a disaster. A trusted reputable local contractor should be sought to operate and maintain the technology.

Lastly, the trust board may decide to include civil society stakeholders who have an interest in public safety, in order to assist with the educational matters which are also part of the project.

5. What public education is required for Cell Broadcast?

People relate to their personal devices very closely, it is an object of pride of ownership for many people, and in particular young people are very attached to their mobile devices.

Abstract notions of how a specific technology works are less interesting than what the user experience will be, but also there are issues to do with privacy of data that are just starting to surface now.

Also, there are a lot of 'Freakers' out there, people whose hobby it is to configure their devices in non-standard ways, so that they can receive, for example, test messages, before they are supposed to.

Therefore it is good to inform customers that test are being performed using the cell broadcast feature, so that Freakers will know and understand what to expect.

Test messages should always contain text which clearly explains the test nature of the message, so that there is no confusion if anyone should pick up the message unintentionally.

In some cases, people will find that when they buy a phone, the feature will by default be switched on and there is nothing for them to do. In which case they at least need to know what to do when the special alert tone sounds, and what it means. On some phones, the alert tone will sound until the user acknowledges it, so they need to be told how to operate their application.

In other cases, the phone will be sent an over the air activation command causing the alert channel to be enabled. I suggest that if so, customers first be sent a SMS text message some time beforehand to tell them what is happening to their phone and why. Normally the changes only come in to force when the phone is re booted, so the text message may explain that to the user.

In other cases, the phone may not be able to handle OTA so the user must enable the alert address manually himself. If so, then an educational campaign needs to be done to inform users how to do this if they choose to participate. If a user has not taken some steps to opt in, then he cannot be considered to be 'participating'.

The fact that Cell Broadcast is 'Passive' and is not 'Tracking' users must be trumpeted very loudly. For many people, the prospect that the government is tracking them is a disincentive to participate. Therefore for each community a reputable and trusted spokesman must be found to reassure users that there is no tracking, no database, nor any other means of knowing the whereabouts or even the identity of a user due to participation in the alert system.

Since kids are the most savvy in these affairs, perhaps tie in with schools and colleges would be a good thing. Get the kids to learn how to activate the service, learn how it works, and give them opportunities to interact with the community by maybe charging a dollar for enabling the feature for those who are unsure how to do it.

There can also be tie in with other media organisations such as the TV weather shows, these people are often trusted, so they can reminding users when a severe weather alert is pending to make sure their cell broadcast is enabled on their phone tonight.

6. Key issues to be negotiated with carriers

- Their reputation with their customer base.
- Legal liability for participation in the programme.
- Technical issues over integration of the technology.
- Compensation.

In most cases, a customer is free to churn to another operator at any whim, so the network put a lot of effort in maintaining the loyalty of the existing customer base. It customers get irritated with a badly functioning alert system, or one which 'cries wolf' more that its worth, the blame will come on the network. So, the network will want to see very rigorous 'due diligence' observed so that messages to be distributed by their network will be authentic, relevant and professional.

As they will not want to be the body taking responsibility for this, they may want another body such as a government ministry to take care of this matter for them. They may define a single source of entry for any alerts, and make the government responsible for any output from that source.

The distribution network will want to be indemnified against litigation in the case that they sent a message that proved to be false, or if due to some technical issue, the message was not delivered to some users. The distribution network will want to be absolved of any responsibility for the contents of any message.
The distribution network may own and operating several different system technologies in several different frequency bands. There may be a mix of legacy systems as well as future systems under full or partial deployment in their territory. For example the company may own and operate GSM, UMTS and LTE technologies which they operate under the same brand.

Each of these technologies has different capabilities and restrictions, so the network may have a view about how much data and in what format they will accept. This may be the same for each network, or may be different for each system technology.
Their choice has impacts along the whole chain, from CBC, Gateway, trust protocol, and front end. It will be very conservative at first, but it is likely that it will become more elastic as confidence improves.
Regarding compensation, the network may seek no compensation, a consideration in kind, a funding mechanism such as a portion of the universal service fund, a one off payment, or an on going fee based on time, or a fee based on usage.
The Gateway unit should be the device which makes these calculations as it is the part which is under the joint administration of all of the stakeholders.

7. Alerts in multiple languages

There are two aspects to this matter, operational aspects and technical aspects.
The distributing network will not be willing to accept any liability for the contents of a message, so very likely they will insist that the originator sends the message in a multi-language format at point or origination. This will prevent any liability for misunderstandings due to mistranslation or omission of a message.
The originating front end unit must be prepared to create messages valid in the languages and fonts applicable to the population to the served. The transmission protocols must be able to keep the integrity of the languages and the gateway units must be able to administer any trust protocol rules which have been decided regarding the handling of multiple languages.
The front end device may solve this problem by having pre-arranged messages decided in advance by a multi-language committee, or by a wizard which derives the messages based on some pre known codes which can be translated, or by operators inputting separate messages in freeform as and when they are translated by the staff.
Cell Broadcast has several ways to identify languages.

- Using the “Coding Scheme”.
- Using separate MIs.

The 3GPP 023.041 V11.1.0 standard (Dec 2011) define two address ranges for alerts. One range for the ‘Local language’ and another for ‘Other Languages’. The strategy is that every phone is sold with CB enabled and channel 4370 enabled by default. In fact the user may not switch this channel off in the USA CMAS system. It is envisioned that the government would send the alert message in the Local language on this channel. If the user does not speak this language, he will at least hear the special alert tone and can get someone to read the message for him.
At the discretion of the originator, the originator may also send on another language, or languages on the second block of addresses. If the user has enabled the second block and also selected the language, the message will be received in the other language soon after the first was received.

Not included in the present scheme (but allowed for by spare address space) are, further addresses, available for other languages which may not be defined on the official GSM coding scheme, such as local tribal languages. There is no theoretical maximum to the number of languages, but since it takes GSM 1.8 seconds to transmit each message, then clearly keeping it to a handful makes sense.

One difficulty is with fonts, GSM terminals can host fonts such as Chinese or Arabic, but many fonts are not supported natively.
However in such cases the population often use a Latinized version of their language when texting. Find out how the local population text each other and use that method, perhaps on an additional address.

8. Deaf and blind

Citizens with handicaps are well supported by their personal mobile devices and often already have the appropriately adapted devices.
If the user is deaf, then the vibrator on the mobile will alert him to a pending message just as with a normal text. In some cases a more persistent and intrusive vibration cadence could be provided on reception of an alert.
Blind users often have text to speech converters on board of the phone, so that the text of any messages would be read out to them. If could be arranged that the speech synthesiser does this without prompting in the case of an alert.

9. Special technical and procedural considerations with multiple operators

We have already mentioned that different system technologies may have different restrictions as to the maximum file size and format that they will accept. The gateway unit can arrange this but it may be that the originator keeps the file to the size acceptable by the least capable technology. The trust protocol process will find this out.
Different technologies may have different methods of separating out the different levels of alerts and information to be sent. For example in Cell Broadcast his may take the form of different Message Identifier addresses. Or it may take the form of IP Multicast address or another method.

Either the originators front end unit must be capable of specifying the method of delivery to the last mile network, or the gateway unit must be capable of deducing the correct address block or coding scheme concerned.
Bear in mind that this may be different from one system technology to the next. For example, the ATIS and the TIA have different address block assignments.
In some cases, the MI address ranges have not been defied, so they will be the subject of local interpretation. This is perfectly OK as long as all parts on the signalling chain can carry the required information.
For example, CAP does not in its present for have a field for defining the requested MI code. This will be needed for some applications.

10. Costs

The costs are:

- Compensation to the network.
- Cell Broadcast feature licence fees to the base station vendor.
- Installation of the CBC and maintenance of it.
- Cost of the Gateway and the maintenance of it.
- Cost of Front End unit and maintenance of it.
- Costs of periodic audit of the whole system.
- Costs of training of the users and administrators.
- Costs of maintaining the trust protocol, by means of periodic revision among the stakeholders.

The exact values will be the subject of negotiation between stakeholders.

11. Risks

There are few risks involved in CB, but going forward, the originators the administrators of the gateway and the distribution networks need to keep a working relationship going despite long periods of inactivity and perhaps acrimonious dispute resolution events if things are not going well. Stakeholders should invest in the success of this relationship.

Previously there was a risk that many new personal devices would emerge that did not have any capability to receive CB, but since ht WARN act in the USA, the industry has clearly taken steps to embed the feature into 2G,3G, and 4G networks, and presumably well beyond for the foreseeable future.

However the government and other stakeholders concerned, need to clearly communicate to the vendors of mobile devices, what their expectation is of behaviour, so that terminal vendors are not confused as to how to interpret the sometimes loose guidelines.

None of this has been done successfully before, so there is a strong likelihood of mistakes, (some of them very embarrassing) occurring in the first few years. To offset this, stakeholders should form an international platform for the sharing of “Best Practices”, so that lessons can be learned and problems quenched.

12. Policy or political considerations unique to CB

Political Jurisdiction is well defined geographically. But the ‘Service Areas’ of networks is often arranged in other ways, which may be more technically pragmatic than political.

For example, a BSC and MSC may have a service area which covers more than one national jurisdiction. In the Caribbean for example, many islands may be run from one switch located in yet another jurisdiction, or one island may have two governments but be served by the same switch.

Fortunately this problem has been foreseen, and solutions have been created to handle this situation.

Regardless of the physicality of the Gateway and where it is hosted, the gateway can be administered on a logical national jurisdictional basis, or within the territory of the state concerned, thus stakeholders have the appropriate rights, able to make determinations regarding jurisdiction on their own sovereign territory and none other.

Once national sovereign law has been respected for that sovereign state, the resulting submission message can now safely be trafficked to the network operating center of the participating distribution network, regardless of the physical location of that facility.

At the network facility, the CBC sends the message to those cells which are within the sovereign territory, and not to any cells which are in the sovereign territory of another state such as that where the facility is physically located.

Large scale natural events such as hurricanes or tidal surges may cross national boundaries. Nature does not pay any attention to our human political borders!

However if so, then trust protocols can decide that originators physically located in one territory can have rights to transmit in their territory only provided the terms of the trust protocol have been met. This may be especially true for weather related events or tsunami alarms for example. Sometimes intervention by human decision makers at a local level may introduce unacceptable latency.

The Gateway unit is capable of 'Punting' an international submission to other gateways for further analysis, so that international messages can flow instantly while national sovereignty is still respected.

The technology was designed for all this, but engineers are not national public policy makers, and so political decision making is needed as part of the trust protocol before such a provision may be made in the gateway.

13. Resolution of CB

In the first phase, CB resolution is down to the size of one Cell, but it will be possible to improve on this at a later phase when bandwidth improves enough to transmit the polygon as part of the message. Then the terminal can use its own location system to determine if it is inside the polygon or if it is outside (and can ignore it).

Regarding the first phase, there are still many factors affecting resolution.

When the company cell planner plans a mobile phone cell, his consideration is not what you may think. Rather than plan for best coverage (as a normal planner would), he needs to plan for best capacity. His main headache is interference from his own base stations which may be very near by.

To keep co-channel interference down, the physical size cells needs to be matched to the capacity of the traffic in that cell. The exact numbers are complex and will depend on the spectrum allocate to the network, the system technology, and the frequency band deployed.

As a result of very close frequency re-use, the network often splits the network cells up into so called 'Hierarchical cell structure', with a pattern of Pico cells, micro cells, macro cells (under laid and over laid), and Umbrella cells.

Typically a Micro cell has a range of about 100 meters, whereas a typical Macro cell has a range near to 3Km. In the most extreme cases, Umbrella cells can have a maximum range of up to70Km.

So in more dense areas, the cells are smaller and the resolution is better, but in rural areas the cells are larger and the resolution is coarser.

Passive geo location is the responsibility of the CBC and works in one of three ways.

- The CBC reads the Cell Data file and observes the location of any antennas. Any antennas inside the polygon are included in the transmission.
- The CBC reads the cell planning tool file and observes which cells have actual coverage inside the polygon. If any part of a cell is inside the polygon, then it is included. This gives a resolution within a single cell, about 1-3 Km or so.
- The CBC reads the Cell Data file and 'Reverse Engineers' the data to synthesise a cell coverage map and then applies the second method.

14. Closed user groups and secure closed user groups

Cell Broadcast has much appeal for the application of communications with and between first responders in the field. Here are some issues.
The first responders may have private radio networks, but if they are off duty they will have them switched off.

First responders working the same event but belonging to different organisations may have different and incompatible communications systems.
The originator of the message may not necessarily know the phone numbers of the first responders in the field, they may be self-selecting group for example Red Cross volunteers, or the group may be so large and dynamic, (for example local government employees, hospital employees, off duty doctors) that keeping an accurate data base is very onerous.
But since CB is a multicast technology, actual numbers of the phones are not needed. For example, if off duty hospital workers are needed, then they could be informed of the CB MI topic for such information. As this is not a public alert channel, then the rules for origination would be different from the public alert system. City employees may not carry their radio at all times, but they can set their own private mobile phone to the specified channel, then they will get the message, but only if they are in the relevant area, (not if they are on holiday a thousand miles away).
In such cases, messages would be transmitted in the clear, not encrypted. So very sensitive information should not be sent this way as the receiving group are self-selecting and you will never know who has received the message (friend or foe).
However another reason for using CB is that it is passive, and therefore not affected by overloads and denial of service events. Since emergency situations nearly always overload networks at the critical phase of the emergency, cell broadcast may be the only way to alert group members.
If the message is going to be very sensitive, the originator can sent the message encrypted. The recipient group would then have applications on their phone or SIM card to decrypt the message, if they belong to that group.
However in this case an administrator must know the identity of the members of the group so that keys can be sent to the members in advance and maintained.
There will be many permutations of these two aspects, and so a hybrid approach blending both methods may be part of a total solution.

15. Acknowledgements

One of the critical aspects of alert messages is the very large scale of the distributions of them. If the scale is greater than 10.5, then the signalling load of call set up for acknowledgements may itself cause a problem that the use of CB was designed to mitigate. Note that the USA CMAS system forbids this for the reason above stated.

Provided that the specified target group is small enough, a message can contain a hyperlink to a WAP/WEB page, a phone number or an SMS reply number. Or a smaller number of phones could be programmed to reply back automatically when a message has been received or read.

If the sender wants confirmation that the system as a whole is working, then another approach can be used. A network of outer loop reporting receivers at strategic locations can receive cell broadcast messages, and then report the date and time of their appearance on the air to the sender. This way the sender can verify that the message was sent to the right place and at the right time.

16. New wireless standards

Currently the 2nd generation GSM technology is restricted by its fixed timeslot structure, and has a very low data rate of 80 bytes per 1.8 seconds.

However in 3G and 4G, the cell broadcast bearer service is carried by the combined downlink packet channel, which has capacity of several megabytes per second. Therefore in the future we can expect that the capacity of CB will rise considerably.

In addition the capability of future mobile devices will improve, so that they will be capable of dealing with streaming multimedia content in real time.

This will trickle upward, and in time, public warning systems will have much greater capabilities than they do now.

However the basic management techniques will be the same, so the knowledge we gain with 2nd generation CB will be very valuable indeed.

Mark Wood, Chief Technical Officer, CellCast LLC, London.

Conict Consultants B.V.
Address Hengeveldstraat 42
3572 KJ Utrecht
The Netherlands

UNDP
R3I Project
procurement.bb@undp.org

Tel. +31 6 28 52 52 80
Date 8 February
2012 Fax +31 87 78 45 878
Subject Response to RFI 170212
Email john.tacken@conict.com

Dear Sir/Madam,

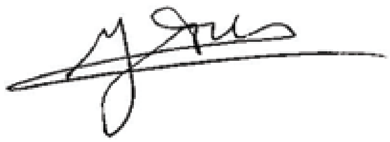
I have noted your Request for Information on the subject of cell broadcast. Conict Consultants B.V. are pleased to provide you with its experiences in this area. We have been the project managers for the specification, procurement, technical implementation and market introduction of the cell broadcast project NL-Alert on behalf of the Netherlands Ministry of Safety and Justice. Subcontractors in this project are the 3 mobile operators Vodafone, KPN and T-Mobile and an ICT integrator. Additionally, I have personally chaired the European working group "Cell Broadcast for Public Warning", where 15 European countries have exchanged information on this subject. https://projectplace.com/pub/english.cgi/0/283748154

We have been involved in this project since 2006 and are able to provide you with experience based information and have limited our response to our specific experiences, having been copied into the response of One2many which contains many technical details.

Please do not hesitate to contact me for additional information.

Conict Consultants BV
Registered Chamber of Commerce Utrecht
under number 30271008
Bank details: ING 4299287

Best regards,



Ir. John Tacken
Managing Director

Answers to RFI questions:

1) What technical steps must be taken in order to implement Cell Broadcast based public alerting?

a. The mobile operators must implement the technical facilities (CBC and network upgrades) to offer cell broadcast
b. An integrator/broker must be able to gather incoming alerts from public authorities, distribute them to the mobile operator (s) and report back on quality of broadcast
c. Public warning authorities must have the technical facilities to enter a message and select a broadcast area
d. Mobile phones must support cell broadcast (important since this is not obvious!)

2) How can the current and forecasted penetration of CB capable handsets in a particular OTC (Overseas countries and territories) be assessed?

We have done this exercise in The Netherlands by testing 90% of the handsets currently in the market, i.e. 300 different types. These test results have to be multiplied with each handsets' market share. Overall result is that 2G phones generally support cell broadcast and in 3G (smartphones) support is poor, but improving in newer models. Overall result in our market was 58% technically capable. Our test results could be used to do the same exercise in a specific OTC. Future penetration is difficult, since roadmaps of handset vendors are kept secret. A scenario analysis is possible.

3) What alert delivery formats are feasible using cell broadcast?

In theory many (bits are bits), in practice only text.

4) Which firms, organizations and agencies must be involved in a successful cell broadcast alert system deployment?

The mobile operators
An ICT system integrator
Handset vendors
A communications agency
Public warning authorities
First responders
Crisis communications experts

5) What public education activities are required in the course of a cell broadcast alert system deployment?

The authorities need to define clear policies in what situations cell broadcast will be used and, based on this, set the right expectations with the public. The public needs to be educated that the service exists, in which situations they could expect a message and how to activate the service on the mobile phone.
Since governments are in most countries the first users of cell broadcast technology, its typical characteristics need to be explained to the public. Especially the difference with SMS.
Experience shows that using the service creates a lot of free publicity.

6) What are the issues which must be negotiated with wireless carriers to implement and maintain a cell broadcast alert system?

We have experienced that mobile operators are very reluctant in offering the service. They fear that cell broadcast will compete with SMS and eat into SMS revenues.
It is important that governments do these negotiations and stress that operators have a corporate social responsibility in offering this service. It also helps to refrain from regulatory measures.

7)What mechanisms are available for providing alerts in multiple languages using cell broadcast?

Within the standards, there are several ways to do this. This should not be an issue.

8)What mechanisms are available for providing alerts to people who are deaf or hearingimpaired, and people who are blind or vision-impaired?

This is easy, since the mobile industry has solved the problem of access of these groups already. Blind and deaf people are massively using mobile phones with tools that enable them to communicate. The challenge is the specific phones that these groups are using (i.e. blind people often use IPhones) often do not support cell broadcast yet. This is a temporary problem.

9) Other than secure provision of the same input (CAP message) to all carriers, are there any other special considerations, technical or procedural, which should be taken into account when planning CB-based alerting in OTCs served by multiple wireless providers?

No

10) What are the various costs involved in deploying?

The costs for The Netherlands were roughly 0,75 euro per inhabitant investment costs and 0,10 cent per inhabitant per year running costs for a resilient, crisis and disaster-proof solution. This includes costs for operators and ICT integrator. For smaller territories, there might be inefficiencies which will make these costs higher. This excludes costs for education campaigns, training, project management.

11)What risks need to be considered in evaluating a cell broadcast alerting deployment?

There are some technical risks with handsets which might hamper deployment. Handset support for cell broadcast is currently sub-optimal, but improving. The main risk though is to set the right expectations with citizens. Firstly as to what to expect from his/her handset. Secondly and more important: to set the right expectations when citizens can expect a message and follow up on this. Sending no information or false information during a crisis seriously affects the citizens trust in the service. The same is valid when sending spam via cell broadcast. In this case citizens will switch it off.

12)Are there any policy or procedural considerations that are unique to CB-based alerting?

There are many. Some examples:
For first responders, the service will be new and provides them with a very intrusive tool to reach many people.

Also most crisis organizations are local. For a de-facto national service, this means there needs to be a national policy for which situations the service will be used or not.
During a crisis, a government gradually gathers the required information for a message. In the beginning, a message will only say that something is going on somewhere. During the course of the crisis, this information will be enriched with an advice on what to do and a reference to follow-up information. The Netherlands expects to use the service during the 'golden hour' after a crisis, after which people will use other media. There will have to be policies as to when, which tools will be used over time during a crisis (cell broadcast, TV/Radio, sirens, crisis website)

13)For localized events, how precisely can the distribution of alerts over cell broadcast be tailored to fit originator specified geospatial boundaries, which may be a priori administrative boundaries or ad hoc bounds developed at the time of an event reflecting a particular set of circumstances (e.g. a "plume model" for a hazardous material release)?

This depends upon the network structure of the mobile operator, the type of network(s) and the number of operators. E.g. in The Netherlands there are 3 operators with 2 networks each (2G and 3G). So there are 6 overlapping infrastructures. Even more complicated: 3G cells shrink and expand their coverage based on the traffic load.
So in general it is difficult to give a clear answer. In densely populated areas, the minimum area is expected to be several (3-6?) square kilometer. In rural areas this might be up to 40-60. But these are very, very rough estimates.

14)In applications for notification of specific personnel, how can cell broadcast be used to notify a particular pre-identified group of individuals (e.g. public safety officers) regardless of their location within the service area?

Cell broadcast uses various channels. A separate channel can be used for closed user groups.

15)How can cell broadcast technology support individual acknowledgement of receipt of alerts and the collection and review of such acknowledgements at one or more operations centers?

The cell broadcast technology as such does not support acknowledgements. That is the reason it is fast and completely privacy-insensitive. It is possible to program a mobile phone in such a way that it acknowledges receipt of a CB message by sending an SMS to a pre-defined number.

16)What changes, if any, can be expected in cell broadcast technology as new wireless standards such as LTE are adopted in future years?

LTE supports a methodology to provide the same service. The best guarantee to get support for cell broadcast in future technologies is that the service is being used by many governments worldwide.
Please note that also the IETF (Internet standardization forum) is working on a standard to broadcast public warning messages via internet technology. So public warning technologies will soon no longer be limited to mobile phones.

A Dutch case study: Cell Broadcast for Public warning, The road ahead.

Willy Steenbakkers
National Crisis Centrum (NCC)
Ministry of the Interior and Kingdomrelations

Communication in Crisis situations

Alarming civilians

Alarming and
Follow up information

Background & Developments
Cell broadcast in the Netherlands

- **2004: Assignment for national government:**

– Find new possibilities to alarm, alert and inform the public in risk and crisis situations, including deaf people and hard of hearing

- **2006: Ministries (MoI and MEA) did research about the possibilities of the technique Cell broadcast**

– Conclusion: cell broadcast is most suitable as communication mean from government to public in civil alert situations

- **2005-2007: MoI, did research about cell broadcast as citizen alert system together with the Technical University of Delft**

Trials in the Netherlands
Questions to be answered

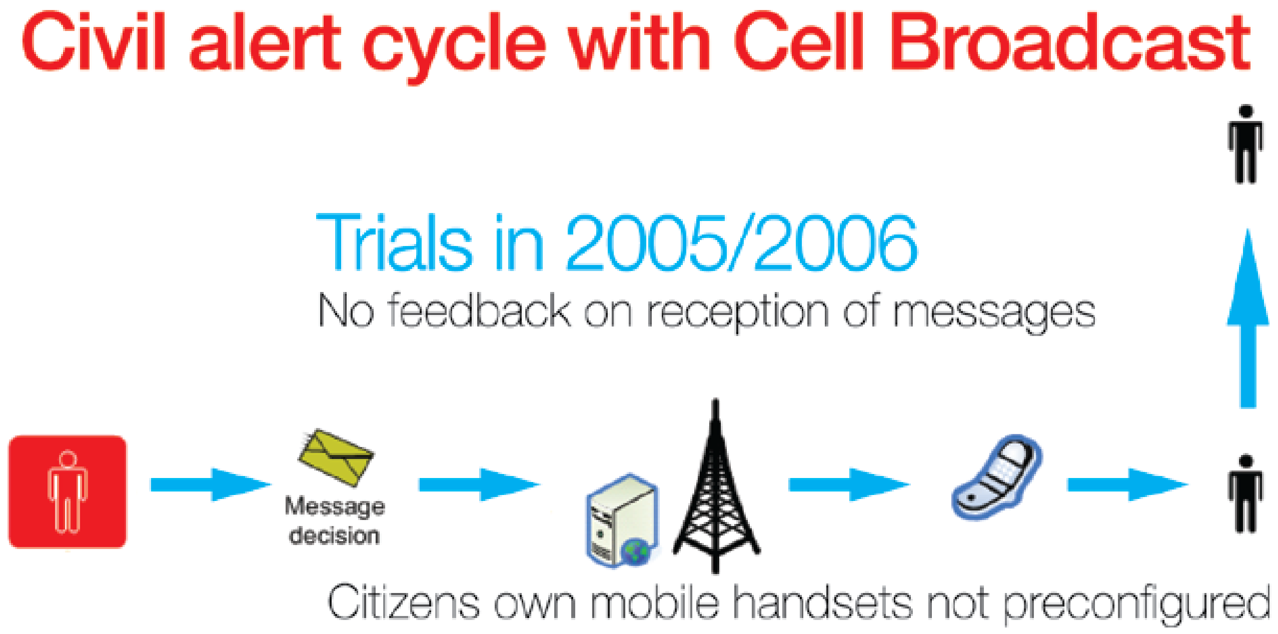
- Cell Broadcast Technology

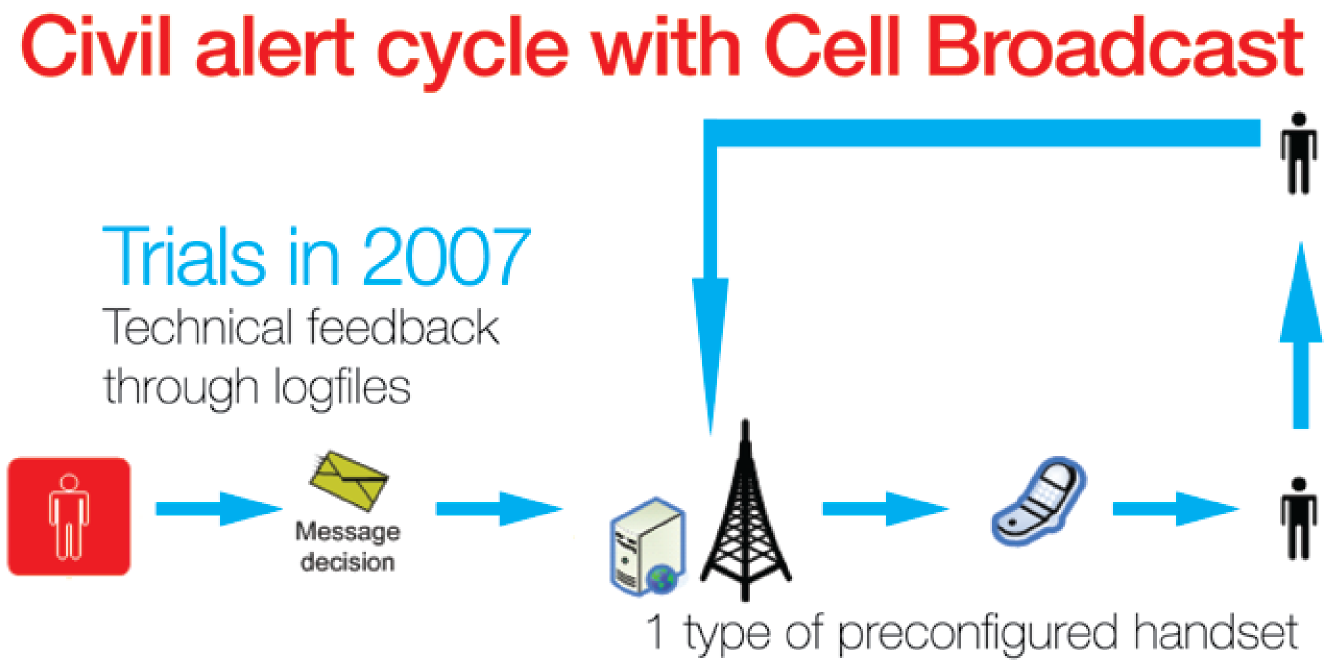
– Is infrastructure at required quality level

- Communication

– How many people can you reach
– The acceptance of the message
– Contents of the message

- Advice and decision


Civil alert cycle with Cell Broadcast
Trials in 2005/2006
No feedback on reception of messages
Message decision
Citizens own mobile handsets not preconfigured


Civil alert cycle with Cell Broadcast
Trials in 2007
Technical feedback through logfiles
Message decision
1 type of preconfigured handset

Results of trials in the Netherlands

- Technology

– Infrastructure can be managed using network management and alignment between government and technology providers
– Setting up the cell broadcast channel can provide problems on mobile handsets

- Communication

– REACH (how many will be reached)
- 86%-94%

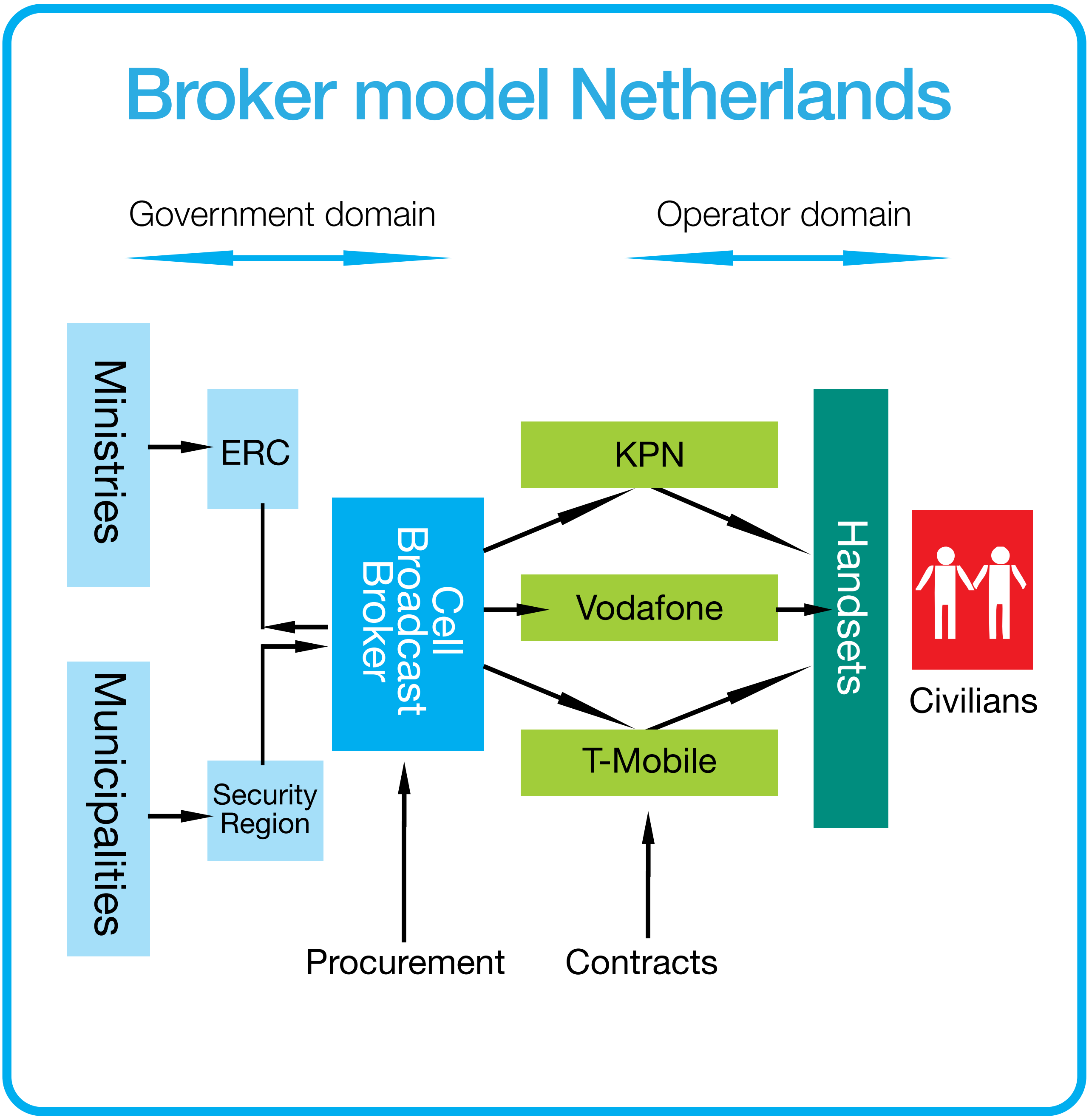
– ACCEPTANCE (of the use as a citizen alert)

- Acceptance amongst citizens is high

– CONTENT (effect of the information)

- Risk, action and information as message content
- Telegram style
- Sender, date and time indication
- Notification should be recognizable: alarm tone
- Advice and decision MoI

– Cell Broadcast is suitable OPT-OUT service for Public Warning
– Start with the procurement`phase of project


Broker model Netherlands
Government domain
Operator domain
Ministries
ERC
Municipalities
Security Region
Cell Broadcast Broker
KPN
Vodafone
T-Mobile
Handsets
Civilians
Procurement
Contracts

EU Project

Exchange of information and knowledge

Standardization in the field of Cell Broadcast (e.g. handsets)

Position paper

Preparation of European wide tests

Grant accepted by EU (JLS)

Partnership countries: Germany, Hungary, Poland, Sweden and the United Kingdom

Participating countries: Austria, Finland, Estonia, Latvia, Belgium, Bulgaria

EU Project
Issues to be addressed concerning cell broadcast

- Threshold for civilians using Cell Broadcast
  - All handsets should support Cell Broadcast
  - User interface on handsets should be standard
  - Keep citizens continuously informed

- Cell Broadcast support on upcoming technologies (UMTS, LTE, Wimax etc)

- Civil alert when crossing the border as tourists (channel allocations, national languages)

- Developing other products in safety and security domain (no commercial applications)

- Cell Broadcast succesfull with citizens acceptance of this new service for alerting, informing and instructing during crisissituations

The road ahead (1)

Strong points of Cell Broadcast

- CB networks are designed to deliver emergency-scale traffic loads
- targeting users in a specific location is possible
- message delivery order is always predictable
- OPT-OUT service (so no subscription like SMS), ‘privacy proof’
- no congestion on network

Issues which have to be decided/developed in the near future

- only received real time if mobile phone is activated
- message may get lost (storage problems)
- long messages not received completely
- ‘spill over’ effect if geographical area is too small

The road ahead (2)

- Start procurement broker (dec 2008)
- Finalize contract with broker (Q2 2009)
- Finalize contracts with operators (Q2, Q3 2009)
- Start building system (Q3 2009)
- First operational pilots (sep 2009)
- System live in the Netherlands (Q1 2010)
- Final Go/No Go decision (Q1 2013)
- After Go decision then contract for 12 years

More information?

- **E-mail**

– cellbroadcast@minbzk.nl

- **Project website about EU-cooperation on cell broadcast**

– https://projectplace.com/pub/english.cgi/0/283748154

– You can also find the lessons from a two-year study in the Netherlands (Report on the use of cell broadcast as a citizen alert system)

One2many response to RFI 20217 Cell Broadcast for public warning

RFI response

Proposed To: UNDP – Regional Risk Reduction Initiative

Proposed By: one2many FZ-LLC

Peter Sanders

Product Manager

Document Version: 1.0

Document Status: Final

Document Release Date: February 2012

one2many

Reaching your audience

Table of Contents

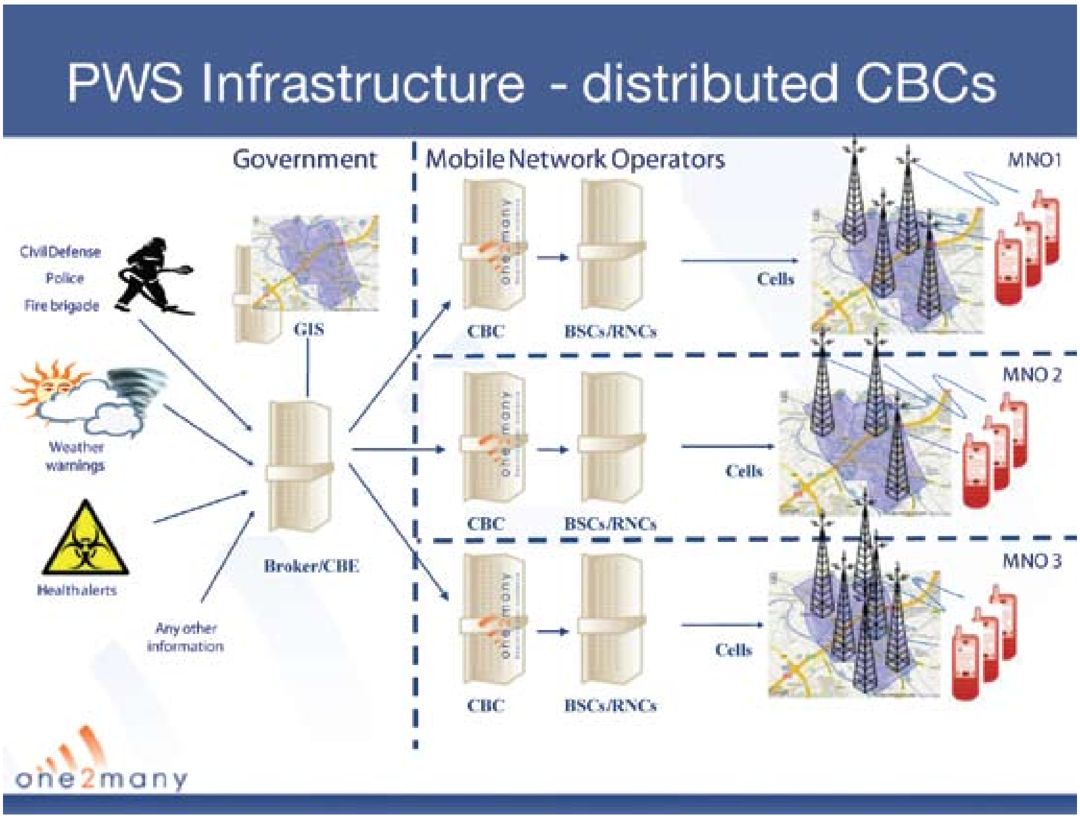
List of Figures

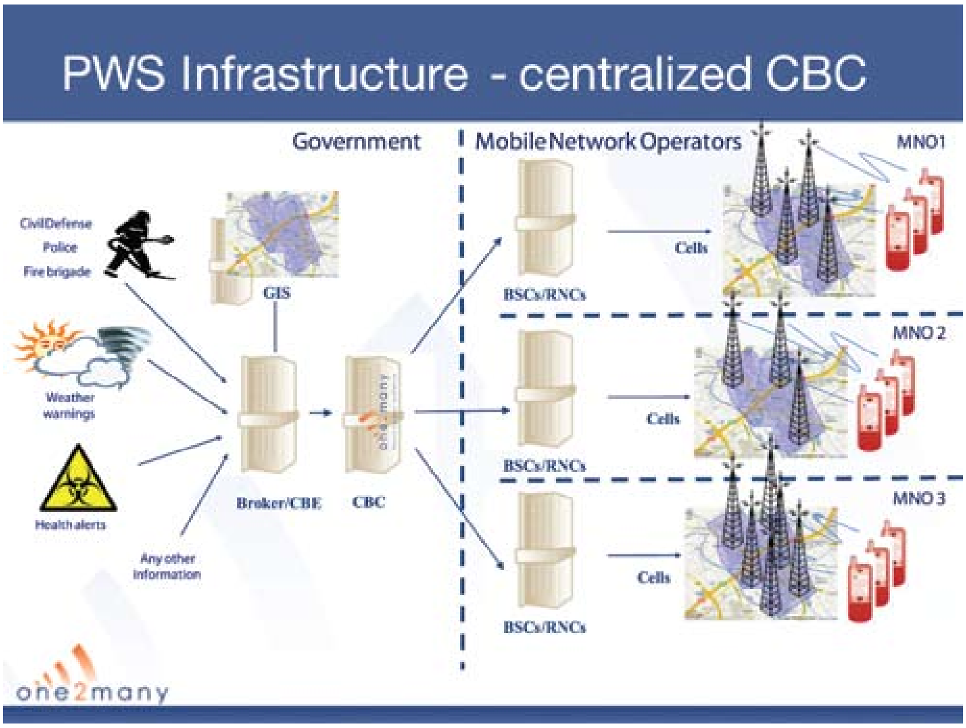
No table of figures entries found.

1. Response to RFI 20217 questions

1) What technical steps must be taken in order to implement Cell Broadcast based public alerting?

The mobile carrier will need to activate the Cell Broadcast (CB) functionality in the Radio Access Network (RAN). This CB feature is supported in all 3GPP type networks. Secondly, the mobile carrier may have to deploy a Cell Broadcast Centre (CBC). Alternatively, the CBC may be a centralized CBC hosted by (or on behalf of) the government. The centralized CBC shall be connected to the RAN of (preferably all of) the mobile carriers via a secure tunnel. Thirdly, a government operated and maintained alert aggregator is required. Alert messages are defined and submitted on this system, and forwarded to the CBCs. On the mobile devices the CB functionality needs to be enabled by the citizens.





2) How can the current and forecasted penetration of CB capable handsets in a particular OTC (Overseas countries and territories) be assessed?

The number of CMAS (US), EU-Alert (Europe) and KPAS (Korea) compatible devices is growing rapidly. CMAS, EU-Alert and KPAS are compatible Public Warning Services (PWS), specified in 3GPP and allow roaming amongst each other. The OTC are advised to deploy a CB service that is compatible with CMAS or EU-Alert. Please refer to the 'background information section' at the end of this document.

3) What alert delivery format (text, audio, images etc.) are feasible using cell broadcast technology?

CB is a text based service but also allows broadcasting of binary files which contain audio or images. In order to extend the support of images and audio, an application on the handset or (U)SIM card is needed to decode and display these binary files.

4) Which firms, organizations and agencies must be involved in a successful cell broadcast alert system deployment?

It is assumed that public warning is a government responsibility and therefore the project shall be driven by the government. The actual messages will be defined and submitted by local crisis management organizations (e.g. fire-brigade or police) and these organizations need to buy into using the system.
The alert aggregator system, and possibly also the centralized CBC, need to be hosted and maintained by the government, or on behalf of the government. The mobile operators need to provide and maintain a CB service capability at an agreed Service Level Agreement (SLA). Citizens need to be made aware of the existence of the service, which may require the involvement of an agency specialized in public communication campaigns.

5) What public education activities are required in the course of a cell broadcast alert system deployment?

Citizens need to be made aware of the existence of the service and what type of messages to expect, and they need help activating CB on their legacy (non CMAS or EU-Alert) mobile device. A website with instructions for 95% of all devices sold in the last few years may help.
Depending on the number of actual alert messages that are going to be broadcasted, it may be needed to do regular tests that include the citizens.

6) What are the issues which must be negotiated with wireless carriers to implement and maintain a cell broadcast alert system?

The wireless carriers need to supply a CB service capability to the government against an agreed Service Level.
For the duration of the agreement, the wireless carriers need to have a support agreement in place with their vendors in order to support the SLA with the government.
Wireless carriers may decide to offer other CB services, however, government alert messages shall have priority over other types of messages; possibly even to the extent that other messages will not be broadcasted at all during the time when an emergency alert is being broadcasted.
Wireless carriers may have to agree to support alert messages not only in 2G and 3G, but also in LTE once that becomes available to them.
The mobile carrier shall sell mobile devices to its subscribers that support CMAS or EU-Alert.

7) What mechanisms are available for providing alerts in multiple languages using cell broadcast?

CB messages can be broadcasted in any language. A parameter of the message is the Data Coding Scheme (DCS). This DCS may indicate the language. The mobile device allows filtering of CB messages based on a preferred language setting in the mobile device. For example, a message can be broadcasted in English, French and Spanish in three separate messages. If the mobile device has a setting to display French messages, only message that have the DCS value set to French will be displayed; the others will be ignored. The default setting is usually ‘all languages’.

8) What mechanisms are available for providing alerts to people who are deaf or hearing-impaired, and people who are blind or vision-impaired?

CB allows broadcasting a text message to a mobile device, quite similar as SMS allows sending a text message to individual mobile devices. Special precautions for hearingimpaired or vision-impaired people are not CB or SMS technology specific, but are specific to the mobile device, like vibration or text-to-speech.

9) Other than secure provision of the same input (CAP message) to all carriers, are there any other special considerations, technical or procedural, which should be taken into account when planning CB-based alerting in OTCs served by multiple wireless providers?

The CAP protocol is not a protocol that can be implemented directly for CB based alerting. It requires an Implementation Guide. The CMAS C-interface is specified as the interface between the government system and the mobile carriers, yet this is also not CAP for good reasons.
The C-interface supports a link-test message to regularly check the availability of the link between the government system and the mobile carriers. This link test is not part of CAP.
The government may require on-line reporting from the CBC at the mobile carrier about the success of the message broadcast, or availability of the CB service. CAP doesn't support any reporting at all, nor does the CMAS C-interface.
The C-interface supports Transmission Control messages from the CBC to the government platform to inform the aggregator not send any messages anymore, or to resume sending messages. CAP doesn't have such a mechanism.
Therefore we propose to the CBC vendor specific CBE interface, in order to maximize functionality. This approach has been taken by the Dutch, Israeli and Chilean government.

10) What are the various costs involved in deploying

Mobile carriers need to invest in a CB capability for RAN licenses and CBC.
The government needs to invest in a message aggregator system.
Maintaining the systems for a number of years needs to be taken into the budget.
The government needs to train the users of the system in how to define the right message that is understood by the citizen and upon which the citizen acts accordingly.
The government needs to invest in a media campaign to educate the citizens, which may have to be repeated occasionally.

11) What risks need to be considered in evaluating a cell broadcast alerting deployment?

There is a risk that citizens do not believe in alert messages when too many messages have been received that are not relevant.
The regional authorities who are going to use the system shall follow the government's policy and not invent their own. This may confuse the citizen.
Preferably all mobile carriers need to participate.

12) Are there any policy or procedural considerations that are unique to CB-based alerting?

CB messages are repeated for as long as the emergency warning is valid. This is done for various reasons. Citizens may enter the target area after the start of the broadcast, or may have been in areas with bad coverage. In GSM and UMTS the CB messages are not received while the mobile device is engaged in a voice call or a data download. The repetition rate needs to be considered. Messages can be defined with an end-time or run indefinitely until they are cancelled explicitly. In CMAS the message validity is limited to 24 hours, but messages may be cancelled before that. This also needs to be taken into consideration.

13) For localized events, how precisely can the distribution of alerts over cell broadcast be tailored to fit originator specified geospatial boundaries, which may be a priori administrative boundaries or ad hoc bounds developed at the time of an event reflecting a particular set of circumstances (e.g. a "plume model" for a hazardous material release)?

CB messages can be targeted per radio cell. The message will be broadcasted in the entire coverage area of each cell, and since it is radio, it will not stop at administrative boundaries. The coverage area of a cell can be some 100 meters and with a maximum of 30 km.

14) In applications for notification of specific personnel, how can cell broadcast be used to notify a particular pre-identified group of individuals (e.g. public safety officers) regardless of their location within the service area?

A message parameter is the Message Identifier (MI). The MI defines the topic, and it is the MI that shall be activated on the mobile device. Special personnel shall use messages with a different MI than is used for the public warning service. By this a private channel for public safety officers can be introduced. MIs above 999 cannot be set from the MMI, so the citizens will not be able to display those special messages.
If the message shall be received regardless of the location, then the message shall be broadcasted in the entire network.

15) How can cell broadcast technology support individual acknowledgement of receipt of alerts and the collection and review of such acknowledgements at one or more operations centers?

CB itself is a broadcast technology. Broadcast is a one-way only technology, and does not support confirmation. However, it is possible that a (U)SIM application is used to send a confirmation back to the network. There is no 3GPP standardized solution for this. Note that during a mass broadcast the network will get congested due to the acknowledgement, worsening the situation.

16) What changes, if any, can be expected in cell broadcast technology as new wireless standards such as LTE are adopted in future years?

LTE supports a Warning Message Delivery service which is based on Cell Broadcast. It offers a similar capability as CB does in GSM or UMTS. To the citizen there is no difference.

one2many
Reaching your audience

Appendix A - Worldwide CB public warning initiatives

Over recent years, governments worldwide came to the conclusion that current public warning channels such as sirens, radio and TV are no longer sufficient.

As people carry mobile phones with them wherever they go using the mobile network as an alert channel is an obvious choice. Cell Broadcast has therefore garnered much interest from governments across the world for emergency alerts services including EU-Alert (Europe), CMAS/WEA (USA), National Message (Israel), LAT-Alert (Chile) as well as the Earthquake Tsunami Warning System (Japan).

EU-Alert - Europe

EU-ALERT, the European emergency alerts system is being standardized by Emergency Telecommunications (EMTEL), a committee formed by the European Telecommunications Standards Institute (ETSI). When implemented, the letters EU will be replaced by characters identifying a particular country (e.g. NL-ALERT for the Netherlands and UK-ALERT for the United Kingdom). This allows each country to configure their own system to meet their specific requirements while incorporating it within a common core specification, thereby enabling pan-European interoperability. The Netherlands is the first EU member state to implement EU-Alert and a number of other European countries, like France and Belgium, are currently investigating the possibility of deploying similar services.

Commercial Mobile Alert System (CMAS or WEA) - USA

Following the Warning, Alert, and Response Network (WARN) Act the US is deploying the “Commercial Mobile Alert System” (CMAS), also known as the “Personal Localised Alerting Network” (PLAN) or in short “Wireless Emergency Alerts” (WEA).

The emergency alerts system has been overseen by the Federal Communications Commission and allows local, federal and national agencies in the US to transmit alerts from the President, the National Weather Service and emergency service organisations. The alerts are sent to participation mobile operators who then broadcast them to their customers, using Cell Broadcast. The CMAS/WEA system has involved collaboration between the Federal Emergency Management Agency, the Department of Homeland Security Science and Technology Directorate, the Alliance of Telecommunications Industry Solutions and the Telecommunications Industry Association.

‘National Message’ - Israel

Israel faces a wide range of public safety threats, from natural disasters to geopolitical violence. Zeev Tzuk Ram Head of the National Emergency Management Authority is on record as saying: “My worst nightmare is that a strong earthquake will catch us unprepared with inability to warn the population and oversee and control the aftermath.” The country’s geography exacerbates this as it concentrates the majority of the population in just 35 per cent of the country’s area, making the population highly vulnerable to disasters. In response to this, the Israeli Home Front Command and the National Emergency Management Authority launched the emergency alerts system. Deployed in conjunction with the country’s cellular operators the alert system will use Cell Broadcast technology.

ONEMI 'LAT-Alert' - Chile

Following the devastating earthquake and tsunami of 2012, the Government of Chile recognised the need to implement a comprehensive alert and notification system to warn its citizens in the event of future disasters. President Sebastian Pineda initiated a review into the available options. This review concluded that a multi-channel alert and notification system was desirable. Cell Broadcast was chosen as the primary alert technology to be augmented with notifications over analogue and digital TV broadcast, radio, sirens and the Internet. Following the President's order the Chilean Sub Secretary of Telecommunications (SUBTEL) issued in an official tender for deployment of Chile's next generation emergency alert and notification system in early 2011. The deployment is now underway.

Earthquake and Tsunami Warning System (ETWS) - Japan

NTT Docomo, one of Japan's leading operators, has offered the Area Mail Disaster Service since November 2007. This Cell Broadcast services delivers warnings for impending earthquakes and tsunamis. Users on the NTT Docomo network are provided with handsets that have a specific configuration menu that allows them to chose whether to receive earthquake and/or tsunami warnings or not. The menu also allows users to select the volume and duration of the ringtone dedicated to emergency messages. The Earthquake and Tsunami Warning System (ETWS) has been standardized in 3GPP (a global telecommunications standardization institute). Other tsunami and earthquake prone countries are looking to deploy similar solutions in the future.

Appendix B - CB public warning standardization

Through its involvement in numerous standardization bodies, one2many is active in driving uptake of Cell Broadcast as a global service and enhancing the applications that Cell Broadcast enables.

ETSI

The European Telecommunications Standards Institute (ETSI) produces globally applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

ETSI is officially recognized by the European Union as a European Standards Organization.

EMTEL

Within the European Telecommunications Standards Institute ETSI a special committee has been formed: Emergency Telecommunications (EMTEL) which addresses a broad spectrum of aspects related to the provisioning of telecommunications services in emergency situations. The following standards have been developed in EMTEL for PWS:

- ETSI TS 102 182, Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies
- ETSI TS 102.900, EU-Alert using the Cell Broadcast Service
- ETSI TR102 850, Analyses of Mobile Device Functionality for PWS
- ETSI TR 102 444, Analysis of the SMS and CBS for Emergency Messaging applications

ATIS

ATIS develops standards and solutions addressing a wide range of industry issues in a manner that allocates and coordinates industry resources and produces the greatest return for communications companies in the North American region.

ATIS is accredited by the American National Standards Institute (ANSI).

ATIS has, jointly with TIA, developed standards, based upon three Reports and Orders issued by the Federal Communications commission (FCC) in regards to the Commercial Mobile Alert System (CMAS). To the general public CMAS is known as Personal Localized Alerting Network (PLAN).

- J-STD-100, Mobile Device Behaviour Specification
- J-STD-101, Federal Alert Gateway to CMSP Gateway Interface Specification
- J-STD-102, Federal Alert Gateway to CMSP Gateway Interface Test Specification

CMAS is a technology independent service. ATIS and TIA have recognized that the only viable technology for CBS would be the Cell Broadcast Service. Therefore ATIS has developed standards for the CMSP Gateway, which is basically a protocol convertor between the technology independent Federal Alert Gateway to CMSP Gateway Interface and the CMSP GW to CBC interface.

- ATIS-0700006, CMAS via GSM-UMTS CBS
- ATIS-0700007, Implementation Guidelines and Best Practices for CBS
- ATIS-0700008, CBE to CBC Interface Specification

• ATIS-0700010, CMAS via EPC PWS Specification
The FCC has mandated the support of CMAS messages in the English language. ATIS is developing standards for the support for messages in the Spanish language.

3GPP

Standards organizations, such as ETSI and ATIS, and others in Japan, Korea, etc. have formed a partnership programme to jointly develop global standards: 3GPP (Third Generation Partnership Programme). The following standards have been developed in 3GPP for PWS:

• 3GPP TR 22.968, Study for requirements for a PWS service
• 3GPP TS 22.268, PWS Requirements
• 3GPP TS 23.041, Technical realization of Cell Broadcast Service (CBS)
• 3GPP TS 48.049, Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification
• 3GPP TS 25.419, UTRAN Iu-BC Interface: Service Area Broadcast Protocol
• 3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
• 3GPP TS 29.168, Cell Broadcast Centre interfaces with the Evolved Packet Core

TIA

The Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industries through standards development, government affairs, and certification for CDMA networks.
TIA is accredited by ANSI.
TIA has developed CMAS standards, jointly with ATIS.
Cell Broadcast in CDMA is standardized in:
• IS-824, Generic Broadcast Teleservice Transport Capability - Network Perspective
• TIA-637-A, Short Message Service (SMS) for Wideband Spread Spectrum Systems
• TSB-58I, Administration of Parameter Value Assignments for CDMA2000 Spread Spectrum Standards
Support, specifically for CMAS has been specified in:
• TIA-1149-1, CMAS over CDMA Systems

one2many
Reaching your audience

Appendix C - About one2many

one2many is global market leader in Cell Broadcast Systems

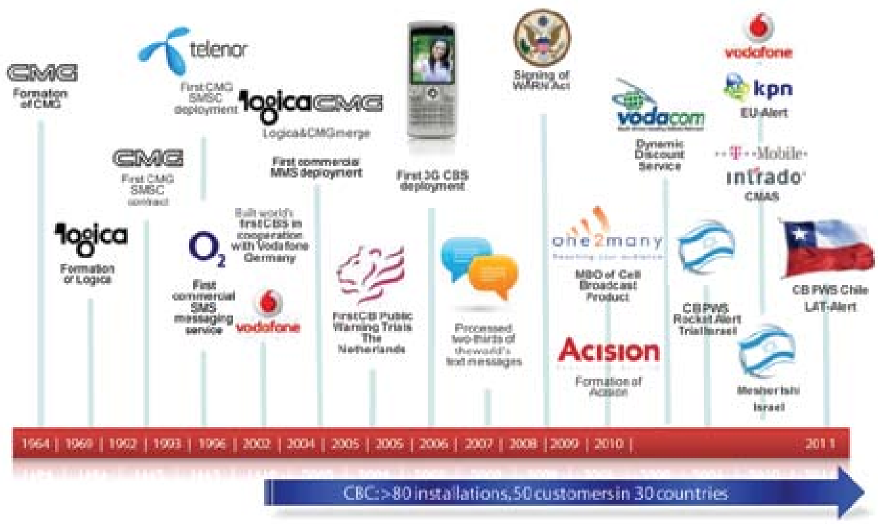
Founded with the ambition to lead the revival of Cell Broadcast, one2many is the only company in the world fully focused on Cell Broadcast solutions. Via a management buy-out of the Cell Broadcast Product Unit of Acision (formerly LogicaCMG Telecom Products), one2many became in one go the world leader in Cell Broadcast, continuing 15 years of experience with over 80 installations, at 50 customers in more than 30 countries.

one2many's proven and stable Cell Broadcast solutions are used over fifteen years by tier 1 mobile operators all around the world for a variety of use cases:

- Public Warning systems
- Interactive revenue triggering services
- Powerful location based SMS-interaction services such as dating and second hand markets
- Dynamic Discount Solutions, broadcasting location- and time specific tariffs to optimize network capacity utilization
- Mobile Advertising Solutions
- And many more

Established in 2007, one2many has its headquarters in The Netherlands, Europe. Employees of one2many are currently based in offices in the Netherlands, Dubai UAE, Serbia, Malaysia and Canada.

The company has close relations with all network infrastructure companies, major SIM vendors, leading handset manufacturers and industry standard organizations, and has a unique combination of both theoretical background and practical field trial experience in CB public warning. This has resulted in the most mature CBS product in the market with its initial release development starting in 1996, and has today the most extensive BSC and RNC driver library in the market. one2many is an active member of standardization committees like ETSI, ATIS, 3GPP, TIA, and the Cell Broadcast Forum and CHORIST (EU project).



1.1 one2many and Public Warning

one2many is uniquely positioned as the leader in utilizing Cell Broadcast systems in Public Warning solutions. For example, one2many is the Cell Broadcast partner in the European Commission funded, 17M€ project CHORIST of an integrated Risk Assessment and Public Warning system.
Furthermore, one2many's Cell Broadcast systems have been the base of the infrastructure for the trials carried out by the Dutch government, involving all Dutch operators and resulting in the use of Cell Broadcast as the new nation-wide Public Warning system.

Last but not least, one2many is an active member in ETSI, 3GPP (ETWS) and ATIS (CMAS) to contribute to the standardization of public warning. Simultaneously we are well positioned to implement the latest standards, including for example the ETWS standards as proposed by Japanese parties in 3GPP.

Our proof points:

- is the most experienced and respected CBC vendor; at customers, handset vendors, network equipment vendors and standardization bodies.
- has more than a decade of experience with over 80 systems installations, at 50 customers in 30 countries.
- has the most mature CBS product in the market, with its initial release development started in 1996.
- has one of the most extensive BSC / RNC driver libraries in the market.
- product design paradigms are based on one2many's most respected SMSC product like high availability, performance and interoperability / open standards.
- has strong company values for social responsibility and business ethics.
- is very actively involved in standardization committees like ETSI, 3GPP, EENA, Cell Broadcast Forum, European Cooperation on CB, and ATIS (WARN Act) / CMAS implementation (US).
- has a unique combination of both theoretical background and practical field trial experience in CB public warning, including in the Netherlands.
- has successfully deployed geographic-redundant CBS systems for Emergency Alert application at KPN The Netherlands, Vodafone The Netherlands, IDF Israel (Bouygues, CellCom, Pelephone), T-Mobile US, Intrado US and Entel Chile.

Building on this proud heritage of assuring innovation, one2many continues to invent, evolve
and deliver solutions that empower our customers to seize new opportunities and success.

Version History

Version Status Date Details of Changes Author(s)
1.0 FINAL 03-AUG-2011 Released document P. Sanders
Document derived from Template Version 3.0 Proposal Template - Full.dot.

Cell Broadcast Technology for Public Warning, R31

Project number: RFI120217

Instrument: United Nations Development Programme (UNDP), for Barbados and OECS

Start date, information delivery: 17/02/12 (and 1/05/12)

Information supplied: Via e-mail procurement.bb@undp.org

Deliverable reference number:	SPMM_01
Deliverable title:	RFI
Version:	1.1
State:	DRAFT: - FOR APPROVAL: - APPROVED: x
Lead of this deliverable:	SPMM consultancy (Stichting Platform Mobile Messaging)
Contact:	W.M.van Setten, director
Email:	wim.van.setten@spmm.org
Other contributing:	- Cell Broadcast Forum – CBF (www.cellbroadcastforum.org) - CEASA – INTernational, Europe (www.ceasa-int.eu)

Contents

1 Introduction

1.1 Scope

This document has been made without any contribution or information exchange with and from the UNDP. It is funded goodwill by the non-for-profit expert organisation SPMM contributing as mentioned for reason of 'good corporate citizen', contribution to the society.
The contributing organisations have in-depth knowledge about the technology and implementation of Cell Broadcasting and the use of Government alerts with Cell Broadcast and complementary digital communication channels. (See Annex)
- The information provided in this document is the sole intellectual property (IP) of SPMM consultancy (Stichting Platform Mobile Messaging).
- It is provided under the terms that all information will be treated confidential and never shared outside the 'United Nations Development Programme (UNDP) for Barbados and OECS', without explicit written approval of SPMM.

1.2 Purpose Of The Document

This document describes the basic answers to the Request for Information RFI120217 Cell Broadcast Technology for Public Warning. The purpose of this document is to give guidance to the use of (cellular) broadcast technology for public alerting in the Caribbean, more specific in Barbados and the OECS.
It will focus specifically on Output 2 of the R31 which focuses on early warning systems (EWS), including the design and pilot development based on the ITU recommended protocol for warning systems, and based on CAP.
Including also the requested key feature of these systems to use multiple simultaneous means of alert dissemination in order to both guard against coverage gaps and technical failures and to provide reinforcement of alert messages to the public.

1.3 Document Versions Sheet

Version	Date	Description, modifications, authors
0.1	8-2-2012	Setup by SPMM
0.2	15-2-2012	Discussion and review by CBF and Ceasa-int Europe, update SPMM
1.0	17-2-2012	Final reviewed and comment document. Updated by SPMM
1.1	1-5-2012	***Censored document version by SPMM***

Table 1: Document versions sheet

2. Reference Documents, Definitions & Abbreviations

2.1 Reference Documents

[1] OASIS. (2005). Common Alerting Protocol v1.1 (OASIS Standard CAP-V1.1 corrected DOM). http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf
[2] The CAP: What, Why and How: http://www.incident.com/cap/what-why-how.html
[3] 3GPP TS 23.041, 'Digital Cellular Telecommunications System (Phase 2)'; Technical Realisation of the Short Message Service Cell Broadcast (SMSCB), version 7.0.0
[4] 3GPP TS 23.038, 'Alphabets and language-specific information', V8.1.0
[5] ISO 639-1, 'Codes for the representation of names of languages'
[6] ETSI TR 102 444: 'Suitability of SMS and CBS for Emergency Messaging'.
[7] Cell Broadcast Forum "CBF-PUB(02)2R2.4", 'Handset requirement specification'
[8] 3GPP TR 22.968 V8.0.0 'Study for requirements for a Public Warning System (PWS) service
[9] Delft University 'Evaluation of the use of Cell Broadcast for citizens warning.'
[10] Chorist_SP3.D55 'Lessons learned by TUD on Emergency Warnings' (www.chorist.eu)
[11] Chorist_SP3.D7 'Personal Communication Networks Gateway technical specification'
[12] Chorist_SP3.D16 'Multilingual aspects in public warning'. (www.chorist.eu)

2.2 Definitions

Alert/alarm Warnings with the goal to initiate behavioural change so as to limit damage to persons and property
Citizens warning All communications (audible, visual or textual) under authority to citizens during the course of an emergency, major incident or disaster
Required action(s) That action or those actions required for citizens to be safe or get in safety in case of an emergency, major incident or disaster

2.3 Abbreviations

3GPP	Third Generation Partnership Programme.
ATIS	Alliance for Telecommunications Industry Solutions
	Broadcast A transmission to multiple, unspecified recipients.
BTS	configuration data Coordinates and, optionally, geographical area that is covered.
CBC	Cell Broadcast Centre
CBE	Cell Broadcast Entity
CBS	Cell Broadcast Service
CDMA	Code Division Multiple Access
Cell Broadcast area	Geographical area(s) to which messages are broadcast. Cell Broadcast areas may comprise one or more cells or entire PLMN.
ETSI	"European Telecommunications Standards Institute".
GeoRSS	Geo stands for Geographic and RSS stands for Really Simple Syndication. In GeoRSS, location content consists of geographical points, lines, and polygons of interest and related feature descriptions.
GSM	Global Systems for Mobiles

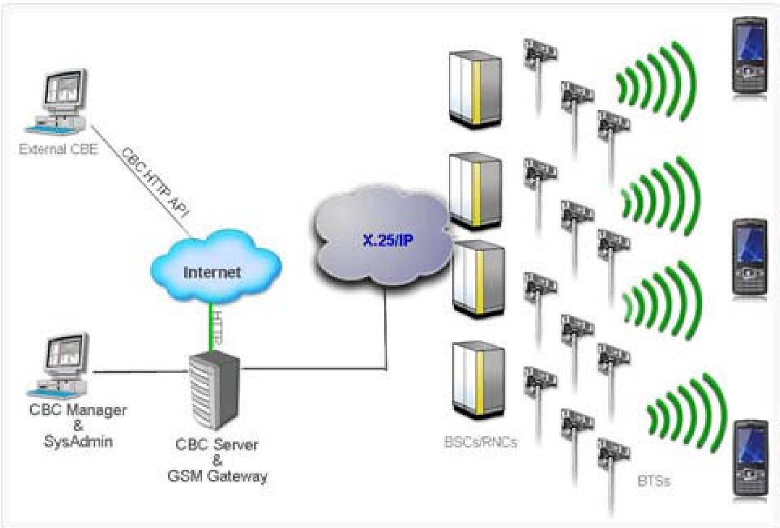
ITU	International Telecommunications Union
MDS	Mobile Device Specification
MS	Mobile Station - the mobile handset
OTA	Over-The-Air
PLMN	Public Land Mobile Network
PWS	Public Warning System
QoS	Quality of Service
SIM	Subscriber Identity Module
SMS	Short Message Service
TIA	Telecommunications Industry Association
UMTS	Universal Mobile Telecommunications Systems
WAP	Wireless Application Protocol
WiFi	Wireless Fidelity. Wi-Fi is a trademark and brand name for products using the IEEE802.11 family of standards.

3. Questions & Answers

3.1 Q1 - What Technical Steps

What technical steps must be taken in order to implement cell broadcast public alerting?
There are three distinct (technical) domains and separate technical steps:
A: The Government Domain
B: The (Mobile) Operator Domain
C: User Domain

Schematic overview of the 3 Domains:
- Government Domain: CBE (Cell Broadcast Entity) use
The Telco can provide a Web based CBE for Governments or commercial dispatchers – which make it easy for starting with CB. More advanced is to use an API, to interface from the Government Alert Centers or Commercial ICT dispatch equipment to the Telco Domain CBC's. This API interface can also be used to have a CAP gateway interface to the CBC.
- Telecom Domain: CBE, CBC and Telco network
- User Domain: Mobile handsets



Courtesy of Celltick

Above a typical Cell Broadcast architecture configuration.
Governments which will use Cell Broadcast messaging can do this via using the CBE (Cell Broadcast Entity).
Although the implementation of both the CBC and the CBE differ from company to company – (almost) all have the same basic possibilities from 1: Selecting an area (Geo/Gis based), 2: Define the message, 3: Define the time – for dispatching a Cell Broadcast message. (Where, What and When)
There are some differences in the reporting, also depending what the operators allow to be reported. This is managed by the CBC manager, in complete control of the Operator (What)

A: The Government Domain is the area where the Government decision making process takes place, supported by (local customized) ICT. In general Governments already have some form of alerting service to the public, in case of emergency.
The new to be implemented technology should respect the existing technology, support or interface with this technology – preferring via secure, open and flexible standards.

The Government Domain technology should support the decision making process existing, especially true in the pilot development phase and at the same time using open and flexible ICT to support in case needed at a later state the adjustments in the decision making process.
Within the Government Domain the Government has the sole unique undisputed, secure rights of the used technology, not to be shared by anyone outside the Government Domain.
ICT systems used within the Government Domain can be build tailored specifically to Government defined specification (and local situation with respect for the installed based used) and delivered as a turnkey system to the Government. They make use of the secure API interface to connect to the Telco Domain.

B: The (Mobile) Operator Domain is the area where the (Mobile) Operators decision making process takes place. In general Operators decide based on their business model whether they will implement Cell Broadcast as one of their Mobile Operator services or not. The telecom network they have in use is the core investment of the operator; the 'wholly grail' and normally (Mobile) Operators do not accept anyone to control part of their network. For an Operator this means that apart from having their network, for Cell Broadcast they have to have the network software for cell broadcast in their systems active (software from Nokia, Ericsson, Nortel etc.)
The Government could contact the (local) Operators and negotiate the use of the (local) Operator network with Cell Broadcast messaging services, with a defined service level.
By providing this Cell Broadcast messaging service Operators have to provide a well defined technical interface to the outside world - as is not uncommon by using other mobile services like USSD or SMS, as provided by Operators to their customers.
To manage the service level and providing a controlled and safe interface to the outer world, to go outside the Operator Domain, normally Operators invest in a Cell Broadcast Centre (CBC). These are systems from organizations designing and marketing CBC's (software from Celltick, Bercut, Silat, one2many, TeleDNA, Bercut, Celltick, Huawei etcetera.)

The interfacing between the two mentioned Domains:
Could be CAP, but not always preferred - The Common Alerting Protocol (CAP) is an XML based data format for exchanging public warnings and emergencies between alerting technologies.
However the interfacing to the CBC's is in general not ready (yet) to use the CAP standard. The CAP uses also quite some overhead, reasons why Operators in general do not prefer to use this as a standard interface.
For the flexibility of the chain it is not mandate to have between the two mentioned Domains a CAP interface, as any other secure standard interface capable of handshaking text based messages will do the job.
The move to use within the Government Domain 'CAP' as the standard way for interfacing various systems makes sense. Interfacing to other digital communication channel systems, different from interfacing to CBC's within the Operator Domain could help limiting the confusion and making it easy to use other Digital Channels of communication, like the channels common used with the social media. (Twitter, rss feeds, blog etc.)
(More in-depth knowledge in the EU Chorist study – www.chorist.eu – authors have been active in.)

C: The User Domain: the citizen in the crises area.
Users use a wealth of communication tools these days. Communication via Radio (DAB), TV (DVB), Fixed line Telephone, Mobile Telephone, (Portable) Computer, IPad, Satellite receiver etc. Since decades the Governments use also siren systems to warn citizen. For the Government it is important that Users can be reached. The Citizen of a country decides whether or not they will and can receive the Government alert messages.
This means that the type of receiver the User has in operation, defines whether the Government can reach the User via Cell Broadcast messaging services, completing the communication chain. (see 3.2)

3.2 Q2 - How The Penetration Of Cb Handsets Assured

How can de current and forecasted penetration of CB-capable handsets in particular OCT be assessed?

1: The good news is: Cell Broadcast is supported on almost all 2G handsets (>95%), mobile telephones and this works as one might expect, proven and reliable. However the user has to select themselves the activation of the handset. There are databases with information available assisting the user in doing so.
Note: There have been and still are experiments to activate Over The Air (OTA) the cell broadcast receiving function of a handset by an operator, as many other services are. In spite of many interesting ideas about this OTA function and cooperation with operators, it is nowhere in the world implemented in a scalable, robust and proven way for mass communication. The specification how this could theoretically work is described in document 3GPP TS 24.012. One of the reasons is that the Cell Broadcast messaging service uses part of the SIM card function and there are different SIM's in use, specific memory size and the UICC (Universal Integrated Circuit Card), also called SIM card. The knowledge what handset is using what type of SIM is not easily available on a mass scale, by operators. At this moment: not reliable and not advisable to implement for mass communication.
It is advised to use databases and web based services for citizen how to activate the Cell Broadcast receiving function of the various handsets available in the market, which works fine for 2G handsets.

2: The not so good news: The operator network could support the transmission of 2G and 3G cell broadcast messaging, but the receivers, the mobile handsets, are not automatically always capable of receiving these messages.

3G: The increasingly popular smart phones using 3G - will NOT display the Cell Broadcast messages (apart from just a few handsets like Huawei etc) – it is in general not supported by the handset, even if the 3G network is transmitting the Cell Broadcast message, which can be done quite well from an operator point of view. This is work in progress at this moment in time.

Dual mode of operation (2G and 3G): Note that smart phones are delivered from the factory (in general) in so called dual mode of operation. In this mode the handset switches automatically and very convenient, from 3G to 2G, if and when there is not a 3G network service available in a certain location. Note however that handsets in dual mode never will receive and display a Cell Broadcast message in this mode, at this moment in time. Not via 2G and not via 3G.

Manual switch (3G to 2G): Note that smart phones can be switched also manual by the user to communicate via 2G and some smart phones (like Nokia, Samsung etc.) are then capable of receiving CB messages via 2G, however by far not all, like the IPhone or Android.

Android and IPhone: Popular Android and IPhone smart phones do not standard support Cell Broadcast at this moment in time, not via 3G and not via 2G. (Note: for the open platform Android there are some non standard supported fixes, which are interim solutions.)

This is a **severe limitation** and the chicken and egg problem implementing Cell Broadcast messaging services in general. This has to be managed in a proper way, from a user's perspective.
There are from authorities and the Cell Broadcast Forum (CBF) in-depth discussions with the handset manufacturers to change this situation. However the business model for Cell Broadcast is not very rewarding, meaning that handset manufacturers are not very enthusiastic to implement on the smart phones per default the CB function and also the Operators are not demanding this function at the top of their priority list of functions to be implemented. This could very well change if and when authorities and operators demand this function from handset manufacturer for citizen alert. Our experience is that this takes 'some time'.
In our view Cell Broadcast messaging services can be piloted quite well, if considered to be used in combination with other mass communication via mobile devices, as an interim solution until the mobile devices support issue for CB, described above is solved.
It is therefore advised to have an interim solution in order to mass alert the citizen, via mobile handsets, especially to make use of **WIFI network** services as an intermediate alternative for 3G or LTE. There are some interesting interim solutions, which might help moving forward. Especially for the Caribian islands, where the population in a certain area is not several millions of people, a push GeoRSS feed can be implemented. With GeoRSS readers (or special Government prepared reader apps for smartphones like Android, IPhone, Symbian and MS) this could be a valuable addition to alert citizen - via their mobile phone.

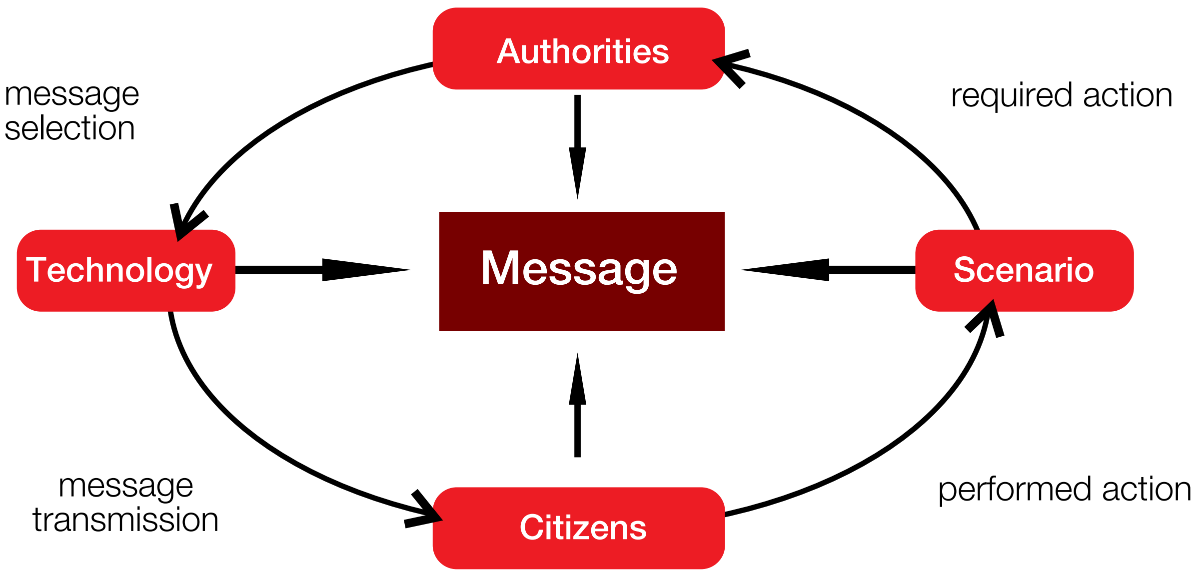
3.3 Q3 - What Alert Delivery Formats Are Feasible?

What alert delivery formats (text, audio, images, etc.) are feasible using cell broadcast technology?
There are general available specifications available for Cell Broadcast messaging: document 3GPP TS 23.041 specifies e.g. how a Cell Broadcast message shall be coded.
Cell Broadcast messaging in practical terms is **for text purposes only,** in many supported languages (most popular languages see specification document Q7) **Binary data can also be used**, for instance for encryption-decryption services or for machine – machine communication via CB.
Cell Broadcast messaging services in combination with specific actions activated in the handset give another range of additional functions. For instance: a sound or siren can be activated on the handset. So the moment a particular CB message is received in the handset an audible alert with light flash could be heard and seen – on a prepared handset.
One other example: using one of the available texts – speech solutions, via cell broadcast to many mobile stations in a geographic area without the need to individually address messages to the mobile stations. This way it is possible to hear spoken messages or instructions.
A quite well supported function is for instance to activate opening a website with Wireless Access Protocol (WAP) push operations or to display a pre-stored picture etc.
Note however that (almost) all of these mentioned solutions require special preparation of (selected) handsets; it is not a common solution for all mobile handsets, for all citizens.
There are pending discussions and growing support by government authorities to have in all handsets an

audible alert siren ‘standard’, however this is also ‘work in progress’.
The safest way to implement Cell Broadcast as one of the channels of mass communication used by Governments for alert purposes is to **focus on text only** – and have in addition for the disabled citizen special prepared solutions on selected handsets.

Construction of messages

Four aspects play a role in the selection and construction of citizens warning messages. These aspects are the emergency scenario, the role and responsibilities of authorities, the technology used for transmitting the message and the citizens that have to receive and act upon the messages. All of these aspects have their influence on the message. (Courtesy Chorist research)



The **scenario** determines the need to alarm or inform citizens about an emergency situation, and therefore determines the basis of the required action. At the same time emergency situations are very uncertain. It is impossible to predict when and where accidents will happen, or exactly how natural disasters will develop. Therefore protocols for dealing with uncertainty usually allow for large flexibility. The level of uncertainty in information that is acceptable in communication to citizens and how uncertainty is treated are issues that need to be addressed.
Even though the emergency situation seems to ask for certain action, the **authorities** have to decide whether they want to send out the message or not (yet). Given the uncertain nature of emergency situations, response to these situations therefore is very much an on-hand process. The communication to the public nowadays is very limited.
The protocols currently in use do not provide much in information or required action for citizens. In terms of communication to citizens authorities embrace the adagio is **KISS**: “Keep It Simple Stupid”.
For in-depth information about lessons learned for Chorist partners, see the document Chorist SP3.D55: Lessons learned by Delft University of Technology on Emergency Warnings.
The messages have to be constructed according to the **Common Alerting Protocol (CAP)** protocol [1]. CAP is an open, non-proprietary standard data interchange format that can be used to collect all types of hazard warnings and reports locally, regionally and nationally, for input into a wide range of informationmanagement and warning dissemination systems.

The recommended message system uses the following information. Some of the information is required, while other items are optional:

1. Label alarm level	(Required)
2. Type of scenario	(Required)
3. Location of the event	(Required)
4. Information on the situation	(Optional)
5. Required action	(Required)
6. Other relevant information	(Optional)
7. Where to get more information on the event	(Required)
8. Sender identity	(Required)
9. Timestamp	(Required)

General syntax of warning messages:
Government <label> <Scenario> <Location> <Information event> <Required action> <Other> <More information> <sender identity> <time stamp>

With Cell Broadcasting the amount of characters used for alert messaging is recommended quite limited, although the technology allows 93 times 15 pages to be transmitted max. In practice less is (much) better – less than two pages (<186 characters) - meaning careful construction of messages is important.

3.4 Q4 - Which Firms, Organisations And Agencies?

Which firms, organisations and agencies must be involved in a successful cell broadcast alert system deployment?

There are three groups of organisations identified: (1) The Mobile Operator(s), (2) ICT service companies and (3) Consultancy Expert knowledge.

1: Local Operator(s)
The Local Operator is capable of delivering a turn key solution for CB messaging services, as part of their total Telco solution portfolio, to be used directly by the operating user, in this case the Government.
By building a Cell Broadcast infrastructure within the domain of the operator a CBC (Cell Broadcast Centre) system has to be selected – from companies (alphabetical order). These companies work together with the network suppliers for special CBC interfacing and certifying their interfacing capabilities to the core network system suppliers like Nokia and Ericsson.
CBC system suppliers:
a: Alcatel – Lucent
b: Bercut
c: Celltick
d: Huawei
e: Netxell
f: One2many
g: Silat
h: TeleDNA

Almost all companies have a CBE for commercial or other use (Government alerts), either as a web based client approach and/or an API interface.
The API interface for the CBC is not standardised in either ITU or ETSI specifications and is dependant of the company implementing. Operators can and will document how the external world like the Government can interface with their service systems, including the security requirements.

2: Government ICT solution supplier
There are at least 3 possible approaches:
A: The Government is using the Operator CBE functionality, out of the box experience, with Operator support for CB Alert messaging. This means that the Operator is also the Government ICT solution provider.
Risk management A: The fall back if all fails - The risk is completely with the Mobile Operator(s), as the Government will contract for a service by the operator. The operator is responsible for their infrastructure including the selected CBC service solution provider (see 1).
B: The Government is using the Operator CBE functionality for CB Alert messaging Government and is customizing the supplied Operator CBE functionality to the requirements, f.i. with a localised web designed screen(s) for Government Alerts or combine one screen for more then one CB channel, which is not very complicated to do as well. The technology remains the same as for A, including the support from the Operator, but with added localisation. Some CB project knowledge is required in the project team.
Risk management B: The fall back if all fails: could easily go with the approach A.
C: The Government wants a full custom approach, build and integrate an alert solution with a Crises Centre, via the Operator(s) provided API interface. Note however that the Operator(s) will be less involved in this approach, much higher risk and in-depth full knowledge of the project team is required.
Risk management: The fall back if all fails: could go back to approach B or A.
Described and explained in more detail:
If and when the Government finds for Alert messaging the commercial available CBE solution acceptable, as can/will be supplied by the Mobile Operator, only some of the shelf hard and software is needed. This will already provide all the ingredients to run a serious operational pilot.
In addition with some limited adjustments / customisation of the commercial available CBE software supplied via the Operators, very rewarding customising results can be achieved. F.i. have a screen layout and design from the Government (with Government logo / colour / available web design style guidelines etc.) for using and dispatching Alert messages. Even procedural integration with existing Crises Centre could be done with using defined procedures and a ‘loosely coupled’ ICT infrastructure.
The added advantage is that (maybe) a local Web builder / Internet solution providers could be involved, stimulating the local community and learn how to work with these new state of art solutions, also good for the long term.
If the Government wants to go beyond the mentioned basic CBE or even the customised CBE solution services and reporting, then Government ICT solution suppliers could be invited, which can and will make use of the API interfacing.

For instance if the purpose is to have a direct fully integrated solution with a Crisis Centre, interface via the secure API with the existing Crises Centre ICT solutions (or even a complete new to be developed Crises Centre), a much more advanced and financial stronger ICT Integrator Supplier has to be selected with a tender process. Also the project is much more complex then the other two approaches mentioned.
This will be the high risk project approach. To limit the risk a number of global ICT suppliers with top ICT capabilities have to be managed based on well defined Customer Requirements, Description of Work and Deliveries.

3: Expert knowledge in the Project Team, as part of the total Government Project team.
In order to have a steep learning curve about the use of Cell Broad messaging services for citizen and limit the amount of financial and PR risk involved, it is advised to have independent available expert knowledge, as part of the Government Project Team involved. The requirements for building the expert project team knowledge is highly depending on the approach selected, as described above.
Expert knowledge: SPMM consultancy / CBF (www.spmm.org)

3.5 Q5 - What Public Education Activities Are Required?

What public education activities are required in the course of a cell broadcast alert system deployment?
The public has to do the effort to switch their telephones 'CB on' for receiving the CB messages. There is database information available, which should be on a website for education purposes how to activate the handsets.
Have on a standard time – for instance every first Monday of the month at 12 o clock – during the operational period (after the initial test period) - a formal test message to the public and test the full chain, including citizen receiving the message.
Special care should be for the non – receiving handsets. For the smart phones a workaround should exists and/or communicate very clear that it will not work. Citizen will call on a Government call centre / service centre for advice if in some doubt. The Call Centre members should have a proper training in order to help.
The public should be aware of the CB messages dispatched. This includes tourist visitors - for instance with Samsung mobile telephones every person will get automatically all the CB messages being dispatched, as different from all other handsets. Samsung telephones (excl. smart phones) have an operation function for receiving Cell Broadcast selected 'all CB channels on'. With the dispatching and constructing of (test) messages this should be aware and taken care of.

3.6 Q6 - What Must Be Negotiated With Wireless Carriers?

What are the key issues which must be negotiated with wireless carriers to implement and maintain a cell broadcast alert system?

3.7 Q7 - What Mechanisms For Multiple Language Alerts?

What mechanisms are available for providing alerts in multiple languages using cell broadcast?
In the 3GPP standard 3GPP TS 23.038, "Alphabets and language specific information" you will find the official language support. The following languages are specified in the standard: German, English, Italian, French, Spanish, Dutch, Swedish, Danish, Portuguese, Finnish, Norwegian, Greek, Turkish, Hungarian, Polish, Czech, Hebrew, Arabic, Russian, and Icelandic.
21 languages can be specified with the DCS, where some 150 are actually needed for all languages specified in ISO 639.
The CBS Data Coding Scheme indicates the intended handling of the message at the mobile handset, the character set/coding, and the language (when applicable). This suggests that the DCS can also be used as a language identifier. The DCS is a parameter of the message, and can indicate which language is used for the message content.
Language encoding: The MS shall support a language filter when the DCS language encoding (0001 0000) is used in combination with a language identifier where the first three characters of the message are a twocharacter representation of the language encoded according to ISO 639 [12], followed by a CR character.

It is usually possible to select a language in the menu of the Mobile Station where the Cell Broadcast function resides. Apart from selecting an actual language it is normally also possible to select 'all languages'.
If a language is selected from the menu of the phone; only messages with that same DCS will be displayed.
Messages with another DCS will be discarded. This makes it possible to broadcast emergency alert messages in various languages with the same Message Identifier.

Note: in the 3GPP standard 3GPP TS 22.268, Public Warning System Requirements contains the requirement that when a terminal has been configured to receive warning messages in the home network, and the user roams in another network which also offers public warning services (PWS), then the terminal shall also be able receive warning messages. However, this does not mean that this is implemented yet in the real world.

Behaviour for different languages:
A solution through the Data Coding Scheme - DCS (see 3GPP TS23.038), requires just one message identifier to support most popular (21) different languages, which can be selected by the handset.
Language encoding: The MS shall support a language filter when the DCS language encoding (0001 0000) is used in combination with a language identifier where the first three characters of the message are a twocharacter representation of the language encoded according to ISO 639 [12], followed by a CR character.
It is believed that NOT ALL Mobile Stations, the mobile telephones, support a language filter, although most of the leading Mobile Station – handset manufacturers have implemented this in a proper way, according to the defined standards.
When making an advice judgement based on the handsets which are available at this moment in time on the market, the use of a language filter is depending on the selection in a proper way by the handset user.
We found that most of the handsets in operation have selected the 'right MI' channel with CB 'switched

ON', also have selected 'All Languages on'.
When this is the case then the language filter is not in active operation. Meaning that if and when multiple languages are transmitted over the same MI channel, the user gets all messages.
The good news is that most handsets store received messages in memory, but it needs some handset user practice to read those messages. A recognizable tone added to the alarm MI channel would additionally help getting the message across to the user.
Most handsets have also a tone function and with the more advanced handsets it is possible to have a special alarm tone with it.

3.8 Q8 – What Mechanisms To Deaf Or Blind People?

What mechanisms are available for providing alerts to people who are deaf or hearing – impaired, and people who are blind or vision – impaired?
There are several kinds of solutions already available as an extended or standard function of a mobile telephone:
- People who are deaf or hearing impaired can use a mobile telephone with vibration and/or light signals selected on. The moment their handset is vibrating and/or giving flash lights they know the receiving of a new CB message. There are (selected) mobile handsets which performs these functions.
- People who are blind or vision-impaired can use a text – speech application, an audible alarm signal and/or a Braille reader.

3.9 Q9 –Other Than Secure Provision?

Other than secure provision of the same input (CAP message) to all carriers, are there any other special considerations, technical or procedural, which should be taken into account when planning CB – based alerting in Cots served by multiple wireless providers?
- Governments want to have (reporting) feedback whether their alerts have been successfully transmitted. This asks for a (geo map) reporting facility not all CBC companies have standard at this moment in time.
- Governments want to be able to send out an alert as small as only one cell. This is not automatically true for all CBC's commercial available.
- Governments want to use various types of maps. This is not automatically true for all CBC's commercial available.
- Governments want to secure that messages dispatched are coming from the authority. There are mechanisms for managing this.
- To be sure that the Alert channel is always available – use a regular 'heart beat' dispatch signal for the total value chain in order to know the functioning of the chain and report accordingly. (Technology)
- The 'exact time' used by operators systems prefer to be exactly the same (Not always true - found out the hard way).
- The CAP standard is quite a new standard and could be changed in some details. If implemented - have the standard followed and check the system being deployed when and if a change is published (procedure).
Using CAP is acceptable and possible with a small subset of all the available instructions, which limits the risks involved.

- It is advised to implement CB messaging alerts in combination with an internet / WIFI mass push GeoRSS feed which can be cost effective support for the CB alert channel. For smart phones users and at the same time, with the same basic technology all the users of the various by internet connected computer equipment.
- It is advised to implement CB messaging alerts in combination with an e-mail notification service for selected authorities – to inform them about the sending of an alert - wherever they are in the world. Note this can also be enhanced with a simple sms service for the same people.

3.10 Q10 - What Are The Various Costs Involved?

What are the various costs involved in deploying CB-based alerting, both initial and recurring, and how may they be estimated?

3.11 Q11- What Risks Need To Be Considered?

What risks need to be considered in evaluating a cell broadcast alerting deployment?

A: The Cell Broadcast receiving and displaying function on most smart phones (including the popular IPhones or the Android) is not implemented or functioning. Citizen will not receive a CB alert message on their mobile telephone – selected in dual mode of operation, for selected 2G and
for 3G operation.
Probability: high
Impact: high

B: The security of dispatching a Government alert message is broken.
Probability: low
Impact: high

C: The activation of the CB receiving and displaying function is not correctly communicated to the public.
Probability: medium
Impact: high

3.12 Q12 – Are There Unique Considerations?

Are there any policy or procedural considerations that are unique to CB-based alerting?
The market and technology for mobile telephony is changing and will change even more the coming few years. The trend is towards more digital IP communication – more data exchange. The implementation of the CB services function when and how this will be done will change over time. The official standards for 3G and LTE have specified the Cell Broadcast function, but the commercial demand and drive for this is quite low.
Important to consider: Cell Broadcast is not a common well known communication means for citizen and for the smart phones there are severe limitations at this moment in time, so special care should be taken for education. Basically the Government(s) is doing the marketing for the Operators by implementing this service as the first one.
One of the other aspects is, that the use of the Alert service is (hopefully) not very often activated as it relates to a disaster happening. So consider for the learning of the citizen an additional service – for instance giving the time, every hour or provide a news flash every day at a defined time, with breaking news flash if it is considered of interest, all via Cell Broadcast. This is an innovative private / public cooperation, but interesting for the local innovation of this technology and in our view interesting enough to be considered implementing, especially with respect to tourists.
Meaning that an alert service could be mixed with special news about the country/city etc. which will improve the acceptance of Cell Broadcast use in the daily lives of citizen.
If and when enriched this CB service with a push GeoRSS feed service (via WIFI) and life website content use will embed the CB function with the acceptable technology services and provides a good way of being accepted and used by the public, industry and government.

3.13 Q13 – How Precisely Can Alerts Be Tailored?

For localised events, how precisely can the distribution of alerts over cell broadcast be tailored to fit originator-specified geospatial boundaries, which may be a priori administrative boundaries or ad hoc bounds developed at the time of an event reflecting a particular set of circumstances (e.g. a 'plume model' for hazardous material release)?
The smallest area where a Cell Broadcast message can be dispatched is the size of a single cell, controlled by the Operator.
The size of the cell is depending on the cell antenna used – this can be very small (meters) with the use of a 'Pico cell' or can be quite wide (multiple km/miles) like a cell antenna covering a highway.
For special events or ad-hoc events where new antenna cells will be installed, it is important that the Cell PLMN register of the operator is updated with the CBC; otherwise the cell cannot be addressed for Cell Broadcast messaging. This is a technical service function normally under the control of the Mobile Operator.
Selecting a defined area could be in a few seconds, if and when used an adhoc polygon mapping selection on a relevant geo map, particular for an adhoc changing plume model. The exact implementation is dependant on CBE mapping function related to the used CBC.

3.14 Q14 – How To Notify A Group Of Individuals?

In applications for notification of specific personnel, how can cell broadcast be used to notify a particular pre-identified group of individuals (e.g. public safety officers) regardless of their location within the service area?
Cell Broadcast messaging for a particular pre-identified group of individuals can be send via a special channel number, and/or if preferred to be a complete confidential channel of communication to this group to use standard available encryption technology used both dispatcher part of the CBE and the receiver which is a prepared handset.

3.15 Q15 – How To Support Individual Acknowledgement Of Receipt Of Alerts?

How can cell broadcast technology support individual acknowledgement of receipt of alerts and the collection and review of such acknowledgements at one or more operation centres?
The cell broadcast technology is one message out and received by many. It is a broadcast – a transmission to multiple, unspecified recipients. It has no standard mechanisms in the 'standard' mobile telephone to give an individual acknowledgement of a received message, without additional application(s) build in.
However, on a cell base an acknowledgement can be given:

1: For an operator there are mechanisms to know whether a specific cell has been used for Cell Broadcast messaging or not – this can and normally should be reported to the CBE user as a real time indicator what the status of the system is. This information should be available in the operation centre.

2: In addition there are possibilities for CB monitors. Every cell can have at least one CB monitor. This CB monitor is a specific application which runs on a dedicated mobile telephone. This CB monitor telephone is connected via IP to a computer collecting information in the field. This gives a very solid answer whether a CB message has been send out successfully and report in detail the receiving data.

Note this is not individual but gives a very good indication that the system itself functions according to expectation.

For further detailed information about the CB monitor: A study, specifications and prototype design has been developed by the author (SPMM) in the Chorist research project (www.chorist.eu) – specific document SP3 Delivery 18. Apart from the private document version, which is at request also available by the author, a public version is available which described this approach in some detail.

The management summary of the Chorist document SP3 D18:

"To test this a prototype mobile phone application (Cell Broadcast Manager) is developed which is able to show the Cell Broadcast messages on the screen of the mobile phone, with the time of reception, the message content, the LAC and the GSM CID (Cell ID) where the message is received.

In order to be able to use the cell broadcast network for alarming purposes in case of natural hazards or industrial accidents we have to be certain that all cell broadcast messages sent to a certain GSM cell are received on time and with the correct message content by all phones in the same GSM cell.

In this document a detailed description is given of the Cell Broadcast Manager development project and its resulting application, the Cell Broadcast Manager.

Aspects which are dealt with in this document are the techniques and tools used in the software development project, the functionality of the application, the target phones, its reporting methods and installation process.

The functionality of the Cell Broadcast Manager contains the following highlights:

1: The Cell Broadcast Manager Application records the reception of cell broadcast messages in the GSM cells of the mobile network.

2: The Cell Broadcast Manager runs on a large number of mobile phones.

This makes it possible to know for certain if and when cell broadcast messages are broadcasted and received in certain cells.

The application shows relevant data, like cell id and used GSM cell broadcast channel, of the received cell broadcast messages at the moment of reception. The content of the received message is stored in a file for later inspection. At the moment of reception of a cell broadcast message an audio tone can be played in order to get the attention of the user.

When the cell broadcast network is used for alarming purposes in case of natural hazards or industrial accidents this application is believed a useful addition to the management and monitoring of the total Cell Broadcast Communication to Citizen Network chain."

3.16 Q16 – What Changes To Be Expected In Cb Technology?

What changes, if any, can be expected in cell broadcast technology as new wireless standards such as LTE are adopted in future years?

The market and technology for mobile telephony is changing and will change even more the coming few years. The trend is towards more digital IP communication – more data exchange.

The implementation of the CB services function when and how this will be done will change over time. The official standards for 3G and LTE have specified the Cell Broadcast function, but the commercial demand and drive for this is quite low.

This might change when more Governments specify Cell Broadcast as the Alert communication channel of their choice.

The network technology is not the limiting factor, it is whether handset manufacturers will build in the Cell Broadcast receiving function in the new smart phones the coming years and this is very much market driven.

4. Annex – Spmm Description

SPMM (Stichting Platform Mobile Messaging) (www.spmm.org) is a not for profit The Netherlands based organisation, with the mission to do research, consultancy and acceptance testing of mass communication systems for Government Early Warning Systems.

SPMM is the initiator and has specified a Multi Operator Warning System pilot to be used by the Dutch Government since 2004. This has been developed, tested and installed in the Dutch Cell Broadcast early warning systems Pilot service, full nation wide from the July 2005 till November 2008. This is being used by multiple departments of the Dutch Government, in order to communicate within three minutes core Government emergency messages. Indepth research about the psychological and technical aspects in the acceptance of citizen have been carried out with the University of Delft during that time. Behaviour of CBC's are studied during that time indepth from Logica (now one2many) and knowledge gained about the CBC from Celltick and Bercut.

SPMM has been active in various consultancy expert roles in the Cell Broadcast project called NL-Alert in The Netherlands as an expert consultant for international exchange of standards, defining the research agenda, building new usecases, review consultancy member etc.

SPMM has been one of the organisations active in the EU Chorist research project Chorist stands for: Integrating Communications for enhanced environmental risk management and citizens safety. Information about the project can be found: www.chorist.eu. SPMM has specified and developed in used during 2006 - 2009 a multichannel message dispatcher system, integrated with Crises Centres and used with Cell Broadcasting but also Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), Siren system, push Rss feeds and supportive website technology. During this period intensive cooperation has been carried out with Vodafone Research in Spain and the French EADS organisation.

SPMM has specified and tested CBE webbased systems for Cell Broadcast operational use in 2010 and 2011 in Turkey, Abud'habi, Kenya and India.

SPMM is active under a MOU with ESA Estec, about the use of Europe Galileo satelite (type of GPS) new technology for mass communication to Citizen by Governments via a Galileo emergency communication channel, to be received by GPS receivers - including mobile telephones with GPS receiving capabilities. Giving state of art new capabilities and added functionality for mass communication.
SPMM is a founding member of the Cell Broadcast Forum (www.cellbroadcastforum.org) for the international coordination of channel numbers and handset specifications.

Address and contact information:
SPMM – Stichting Platform Mobile Messaging
Planetenweg 5
2132HN Hoofddorp
The Netherlands
E-mail: info@spmm.org
Website: www.spmm.org
Contact: Wim van Setten (m: 031- 652684166)
Via e-mail: wim.van.setten@spmm.org

Request for Information RFI 120217

UMS is a Norwegian company that provide EWS systems based on different types of technologies for mobile devices, CB and LBAS (Location Based Alert Systems), in addition to fixed lines, sirens, TV, radio, social media and inbound/outbound CAP.
The CB features are answered from one of our partners, one2many, directly. LBAS as an alternative or a supplement to CB is described below and in the attached document.
UMS has implemented CB based warning in the Netherlands and Location Based Alerting based on Advanced – SMS (differ from ordinary SMS in its way of handling speed, congestion, and priority) in Norway. To evaluate which of the two systems that is the most appropriate for each case we use our requirement matrix:

Functionality	
Localisation accuracy	Weather the channel has a localization feature, able to identify the handsets within an area and the level of accuracy of it
Logistics (National)	The capability to provide logistics/number of national handsets within an affected area
Logistics (visitors from abroad)	The capability to provide logistics/number of roamers from abroad within an affected area
Repete	The capability to distribute the warning message in certain given intervals. The content may changed or unchanged
Response	The capability to handle response as a reply to the alert message from the end user
Follow up (to certain different respondents)	The capability to send multilingual warning message according to the nationalities within the affected area
Multilingual	The capability to send a follow up message to affected people in similar situation/similar needs/responded equally
Opt-in/opt-out (subscription)	The capability for the channel/bearer to handle opt-in/opt-out (subscription) in a easy and user friendly way
Real time confirmation of messages sent	Real time status showing number of messages tried sent during the alert process
Real time confirmation of during messages delivered	Real time status showing number of messages successfully delivered the alert process

Cost	
Cost related to infrastructure	Cost related to infrastructure includes hardware and infrastructure investments necessary for the service providers to establish the service
Cost related to implementation	Cost related to implementation includes processes and activities neces sary for the end users (citizens) to take the alert service in use. This is covering both technical and non technical issues
Cost related to maintenance	Cost related to maintenance includes costs necessary for the service provider to run and maintain the alert channel

Network	
Theoretic capacity	The meaning of theoretic capacity is to identify which channel has the best theoretic capability to broadcast a large number of messages in a short period of time.
Practical capacity	The meaning of practical capacity is to identify which channels has the capability to reach citizens within a certain limit of time no matter size of area
Congestion sensitive	Handling congestion is an evaluation of the alert channels capability to avoid or handle congestion in the mobile network
Core network impact	Core network impact is an evaluation of to what extend the annel/bearer is loading the central core system like Visitor Location Register (VLR), Home Location Register (HLR), Mobile Switching Center (MSC).
Air interface impact	Air interface impact is an evaluation of to what extend the Channel/bearer is loading the radio interface and its channels like Single Dedicated Control Channel (SDCCH) which is crucial for the transmis-sion of SMS.
Network protection feature	The capability for this channel/bearer to prevent traffic peaks from causing congestion during emergency situations. This is an add on feature not part of the channel
Authentication	Authentication of the message
Capability to adapt to future generation networks	The capability for the mobile service to follow the mobile evolution, not being part of a proprietary path

Media	
Enabling of other channels	Enabling alternative channels means that once the Mobile Station Integrated Services Digital Network (MSISDN) is available alternative channels like voice and WAP Push may be used (for particular groups). This is not related to the channel/bearer technology itself, but to the addressing method used by the bearer/channel
Text	MMS supported as alternative alert channel
Voice	Voice supported as alternative alert channel
SupportingWAP Push	WAP Push supported as alternative alert channel

Handset	
Supporting all 2G phones	Are all 2G phones with no exception supporting the channel/bearer?
Supporting all 3G phones	Are all 3G phones with no exception supporting the channel/bearer?
Handset chganges required	Is the propagation of the service depending on changes on the handset level which require changes in current standards?
Battery consumption affected	Will the battery consumption increase when enabling the service?
Consistent user interface	Do all cell phones receive the alert message consistently?
Manual config. Required	Does the end user need to perform any activity to activate the alert channel on the handset?

Coverage / Efficiency	
Alert of elderly	Capability to alert elderly without use of any proprietary handset or device
Alert of blind people	Capability to alert blind people without use of any proprietary handset or device
Alert of hearing disabled	Capability to alert hearing disabled people without use of any proprietary handset or device
Alert of visitors from abroad	Capability to alert visitors from abroad without use of any proprietary handset or device
Alert of citizens abroad	Capability to alert travellers abroad without use of any proprietary handset or device
Alert at night	Capability to alert at night without use of any proprietary handset or device

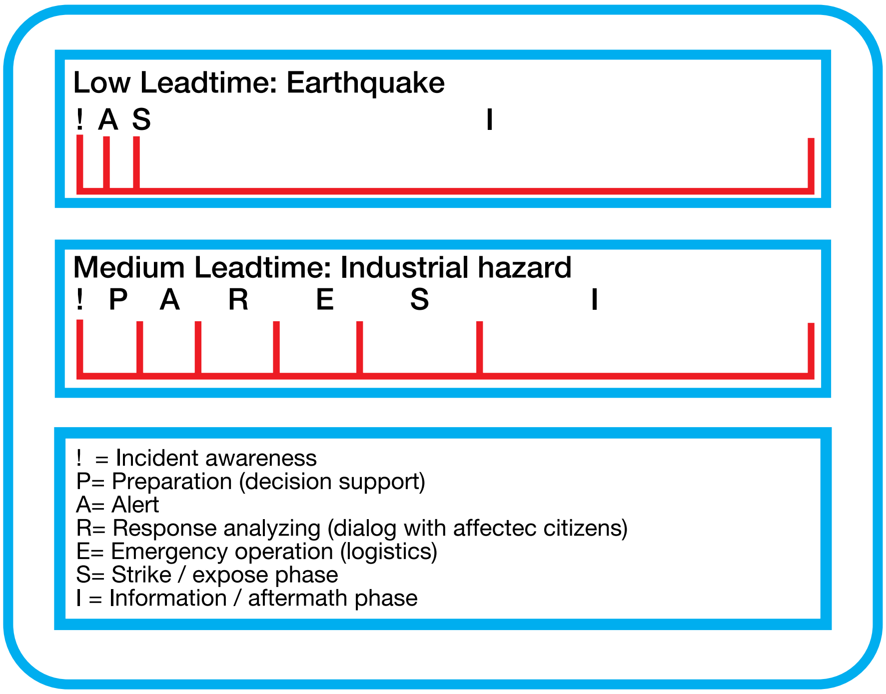
Implementation	
Expected propagation year 1-3	Expected level of propagation during the first 3 years. Manual configuration of hand sets, opt-in requirements or any other activity required by the end user will have a severe impact on this topic.
Expected propagation year 4-6	Expected level of propagation during the next 3 years.
Depending on international propagation	Particularly related to the capability to alert visitors from other countries roaming to national service providers
End user education required	Legislation differs from country to country and must be handled nationally, but nature of the different technologies may require different approaches.

Privacy Issues
Effecting privacy legislation

Handset (For mobile network based PW Systems)	
Supporting all 2G phones	Are all 2G phones with no exception supporting the channel/bearer?
Supporting all 3G phones	Are all 3G phones with no exception supporting the channel/bearer?
Supporting 4G/LTE entities	Are the system prepared to support phones and other devices using the upcoming 4G/LTE channel/bearer?
Support all LTE phones	With this technology coming up. It is important bto ensure the handset regulation includes those devices as well.
Handset changes required	Is the propagation of the service depending on changes on the handset level which require changes in current standards?
Battery consumption affected	Will the battery consumption increase when enabling the service?
Consistent user interface	Do all cell phones receive the alert message consistently?
Manual config. Required	Does the end user need to perform any activity to activate the alert channel on the handset?

This matrix is used when mapping the overall risks that the individual country or region is exposed to.

The "event alert notification time" will depend of the threats that each country or region faces. This could be anything from an earthquake to several less time critical incidents such as flood, storms, extreme temperatures, industrial hazards etc.



UMS is providing pilots according to the results of these mappings.

For your information, UMS has agreed a meeting with UNDP in Geneva 27/2 kl 13.30-14.30 –with Mr. Carlos Villacis, to further discuss possible options.

Please also see enclosed a broader description of the Location based technology that is and alternative or a supplement to CB.

Regional Risk
Reduction Initiative

Empowered lives.
Resilient nations.

This project is financed by the EU and implemented by UNDP