A Report for

Direktoratet for Nødkommunikasjon

Nødnett - Market Analysis Technology

12. December 2008
Engagement: 222433471

Gartner

Table of Contents

Executive Summary

Sammendrag på norsk

Stortinget besluttet i desember 2004 å realisere et første utbyggingsområde av et felles digitalt radiosamband for nød- og beredskapsetatene, basert på TETRA teknologi.

Det er lagt opp til at det første utbyggingsområdet rundt Oslo regionen skal stå ferdig i begynnelsen av 2009.

Det ble også gitt fullmakt til å inngå kontrakt på utbygging av resten av landet, men med forbehold om at landsdekkende utbygging ikke kan igangsettes før evaluering av første trinn er gjennomført. Denne rapporten bidrar til denne evalueringen

Valg av teknologi er kritisk ved investering i infrastruktur. Dette skyldes at den innebærer store investeringer og at andre investeringer vil være avhengig av dem.

Teknologien bak infrastruktur løsninger utvikler seg hele tiden. Typisk vil nye generasjoner infrastruktur teknologier se dagens lys og tas i bruk, samtidig som foregående blir alminnelig utbredt og eldre teknologier fortsatt utnyttes.

Dette scenario er spesielt synlig innenfor telekommunikasjon og radiosamband for nødkommunikasjon.

I denne rapporten stilles derfor spørsmålet; Er TETRA i 2008 det beste teknologi valget for å understøtte et landsdekkende radiosamband for nødkommunikasjon i Norge?

Basert på det teknologiske landskapet med standarder, leverandører og eksisterende infrastruktur kan dette spørsmålet kan brytes ned i tre deler:

1. Vil det være mulig å løse behovet for operasjonell kommunikasjon for nød- og beredskapsetatene med samme trådløse teknologier som benyttes i det offentlige rom som f. eks. GSM og 3G?
2. Vil det være mulig å løse behovet for nød- og beredskapsetatene med bruk av eksisterende offentlig infrastruktur basert på GSM/3G/CDMA EV-DO?
3. Finnes det andre teknologier utviklet for operasjonell kommunikasjon i nød- og beredskapsetater som burde velges i stedet for TETRA?

Svaret på alle disse spørsmålene er: NEI

Vedr. spørsmål 1:

Gartner vurderer hele tiden utviklingen av ulike teknologier i telekommunikasjon markedet. Selv om det i teorien er mulig å benytte teknologier som GSM/ 3G etc., for å bygge dedikert infrastruktur for nød- og beredskapsetatene vil dette uten tvil bli mer kostbart, medføre høyere risiko i utvikling som ikke tidligere er utprøvd og den norske stat vil sitte igjen med en unik infrastruktur uten å kunne dele investeringen med andre.

Vedr. spørsmål 2:

I teorien vil det å kvitte seg med en dedikert infrastruktur for radio samband i nød- og beredskapsetatene være en god ide da man kan utnytte eksisterende investeringer i infrastruktur. I praksis derimot, har Gartner aldri sett at denne ideen har fungert. Det er en rekke uløste problemer for å imøtekomme kravene som stilles fra nød- og beredskapsetatene som f. eks. rask call-setup, høy tilgjengelighet og understøttelse av gruppeanrop. Norge ville dermed blitt det eneste landet i verden med en nasjonal infrastruktur for nødkommunikasjon, basert på et kommersielt nettverk.

Vedr. spørsmål 3:

Det finnes tre signifikante teknologistandarder for digitalt radiosamband for nødkommunikasjon. TETRA, TetraPOL og Apco P25. Alle disse tre standardene vil kunne møte de essensielle kravene for operasjonell nødkommunikasjon.

- Valg av TetraPol resulterer i at man velger en teknologi med bare én infrastruktur leverandør. Denne leverandøren ikke har utført noen større leveranser med TetraPol siden en kontrakt med tre brasilianske regioner ble tildelt i 2005. Spania var siste europeiske land som valgte TetraPol i 2000.
- Valg av Apco P25 betyr at man velger den ledende teknologi standarden fra USA, som ikke har noe fotfeste i Europa og lite fotfeste i resten av verden. Det finnes ingen leverandører som aktivt markedsfører Apco P25 løsningen for nødkommunikasjon i Europa. Det vil derfor være svært utfordrende å finne kunnskap og kompetanse til å rulle ut et slik nettverk.
- Det finnes ingen klare indikasjoner på at det vil koste så mye mindre å bygge ut et Apco P25 basert nettverk sammenlignet med TETRA, at det vil oppveie kompleksiteten og risikoen ved å bygge ut nettverket i Norge.

Gartner har sammenlignet kravene til Nødnett med de kravene andre land har stilt til sin nødkommunikasjon (Danmark, Sverige og Tyskland). Konklusjonen er at disse kravene er samsvarende.

Gartner har også gjennomført en undersøkelse blant beslutningstakere for å få klarhet i hvilke krav de ville stille til infrastrukturen hvis de skulle investere i dag. Også disse kravene er sammenfallende med kravene til Nødnett.

Hvis Norge i 2008/09 skulle gå til anskaffelse av en løsning basert på de essensielle kravene for operasjonell kommunikasjon, ville det beste valget fortsatt være TETRA infrastruktur.

Gartner forventer at kommunikasjonsbehovet for nød- og beredskapsetatene vil utvikle seg utover de eksisterende behovene. Dette inkluderer bl.a. overføring av bilder og video data mellom ambulanser og sykehus og mellom politi biler og politi stasjoner. Dette inkluderer også mobile kontorer for politi.

Dette betyr at nød- og beredskapsetatene vil ha behov for høyere båndbredde enn det TETRA eller andre spesialiserte radiosamband for nødkommunikasjon kan tilby. Det mest sannsynlige utfallet for å løse dette, vil være å utnytte kommersielt tilgjengelige tjenester som 3G infrastruktur basert på WCDMA og CDMA EV-DO.

Executive Summary

In December 2004, the Norwegian government decided to start build-out of a national digital radio infrastructure for public safety based on TETRA technology. Initially, build-out has been started in an area around Oslo, which is currently planned to finish early 2009. The national roll-out was conditioned on a thorough evaluation of the network after build-out of the initial area. This report contributes to that evaluation.

One of the critical decisions in any infrastructure investment is the choice of technology. This is mainly because it typically constitutes a large investment and because other investments depend on them.

Technologies for infrastructures constantly evolve and typically, new generations of infrastructure technologies are visible and on their way as the previous generation are reaching mainstream use and older generations are still alive.

This is certainly the case in the world of telecom and radio networks for public safety.

The issue analyzed in this report is therefore: in 2008, is TETRA the best choice of technology for supplying a national radio network for public safety in Norway?

Given the landscape of technology standards, vendors and existing infrastructures, this question can be broken down into three:

1. Would it be feasible to solve the operational communication needs for public safety organizations with the same technologies as we do public wireless networks such as GSM and 3G?
2. Would it be feasible to solve the needs for public safety based on existing public GSM/3G/CDMA EV-DO) infrastructures?
3. Are there other technologies designed for operational communication in public safety that constitute a better choice than TETRA?

The answer to all three questions is: no.

Ad. 1 Gartner is constantly tracking the evolution of technologies in the telecom world. While it is in theory possible to use technologies such as GSM/3G, etc. to build a dedicated infrastructure for public safety, this would almost certainly be more expensive, involve a lot of high-risk development not proven anywhere, and leave the Norwegian government with a completely unique infrastructure without any other users with whom to share the investment.

Ad. 2 Getting rid of a dedicated infrastructure for public safety radio communications altogether is in theory a compelling idea that would share the investments in infrastructure with a lot of other users. In practice though, the idea has not been proven to work anywhere known to Gartner. There are a lot of unsolved problems about meeting the requirements from public safety, i.e. short call-setup times, high availability, support group calls, etc. Norway would therefore be the only country in the world with a national infrastructure for public safety communications based on a commercial network.

Ad 3. Currently there are three significant technology standards for digital public safety radio communications: TETRA, TetraPOL, and Apco P25. These three technology standards could all meet the essential requirements for operational public safety communication.

- Choosing TetraPol would be a choice of technology with only one vendor of infrastructure and no major contracts since a contract awarded in 2005 for three Brazilian regions. Spain was the last European country to choose TetraPol in 2000.
- Choosing Apco P25 would mean choosing the leading technology standard in the USA, however with no traction in Europe and little traction in the rest of the world.

There are no vendors actively marketing Apco P25 based solutions for public safety in Europe. It would therefore be very difficult to get skills and knowledge to roll out such a network. There are no indications that building out an Apco P25 based network would cost less than one based on TETRA that could offset the major complexities and risks involved in rolling it out in Norway.

Gartner has compared the requirements for Nødnett with requirements stated for other recent networks like Nødnett, in Denmark, Sweden, and Germany. The conclusion is that these requirements are in line.

Gartner also performed a survey among decision makers in this area to determine their requirements were they to invest in an infrastructure for public safety today. Also the requirements that came out of this survey are in line with the requirements for Nødnett.

Therefore, in 2008/2009 was Norway to procure a solution based on the essential requirements for operational communication the best choice would still be a TETRA infrastructure.

Gartner expects the communication needs in public safety to evolve over the coming period. The needs include transferring image and video data between ambulances and hospitals and between police cars and police stations. It also includes mobile offices for Police officers.

This means that public safety will require more bandwidth than can be delivered by TETRA or any other dedicated public safety radio network. The most likely scenario for solving this is to use commercially available services such as the 3G infrastructures based on WCDMA and CDMA EV-DO.

Report

1. Background

The Norwegian government is to evaluate the initial rollout of a national radio infrastructure for public safety (Nødnett). The evaluation should form the basis for making a decision to proceed with a nationwide rollout of the infrastructure. As part of this work, the Norwegian government wishes an evaluation of the TETRA technology on which the infrastructure is based.

The Nødnett project has therefore asked Gartner to investigate the following questions:

1. What are the key communication requirements for public safety organizations?
2. What are the technology options and standards that meet the key requirements of public safety organizations, including use of public networks?
3. Alternatives to TETRA?
    - To what extent is other technologies and standards than TETRA being used for communication within public safety organizations and what is the key market trends for those
4. Evaluation of TETRA
    - What countries have TETRA in operations or are planning to roll out TETRA for public safety organizations communication and what are the key market trends?
5. Based on the functional requirements for the Norwegian Nødnett and other key communication requirements for public safety organizations: Are there any realistic alternatives to continuing the TETRA roll out in Norway? As part of the analysis, availability, cost and risk of handheld and vehicle mounted terminals should be included.

This report documents Gartner's work on analyzing the questions.

2. Methodology

For the analysis of the issues stated above, Gartner has applied the method of hypothesis-based problem solving. For each issue, hypotheses are formulated as well as key questions that will confirm or disconfirm the hypotheses.

Data has been gathered from a number of sources:

- Gartner's vast amount of data and analyses of technologies, including a database of all major telecom contracts, forecasts of market developments for technologies, etc.
- Analysis of publicly available documents on requirements for public safety radio network, status of rollout projects etc.
- A survey among decision makers for national public safety radio networks
- Interviews with decision makers and experts on status and experience with the use of TETRA and other public safety radio communication technologies.

The analysis has been performed by a combination of Gartner analysts and Gartner consultants. Gartner has around 100 analysts covering different aspects of telecom. The Gartner consultants involved in this project brings experience from involvement in a number of large public safety radio infrastructure rollouts in Europe and USA.

2.1. Definitions

Public Safety Organisations	Organisations involved in public safety. The primary elements are Police, Fire, and Ambulance but include also other support organisations. The focus of this report is Police, Fire, and Ambulance.
PSTN	Public Switched Telephone Network
Command & Control Wireless Network Infrastructure (CCWNI)	A communications infrastructure dedicated to operational communication (command & control) in public safety organisations. Nødnett as well as RAKEL in Sweden and SINE in Denmark are all examples of national CCWNI's.

3. Requirements for public safety Networks

Public safety organizations have a special role in society, because they need to work when other aspects of society is not. This is in cases of fires, natural disasters, terrorist attacks, large traffic incidents, etc. Operating in these situations also involves communication under special circumstances. Some of the important characteristics of public safety communication are:

- Public safety people operate in all environments from high-rise buildings in densely populated city areas to uninhabited hills.
- They operate in critical situations from shootouts to bombings to major fires, where communication needs to be instantaneous. Spending a couple of seconds focusing on making a phone call may be lethal.
- They operate in catastrophes were infrastructures for electricity and communication may collapse. Therefore, being able to communicate despite collapse of these infrastructures could be of vital importance to saving lives or catching criminals.
- They operate in situations where a large number of people need to work in a coordinated manner in extremely stressful situations.

Traditionally, public safety personnel has been using analogue radio systems, known as PMR (Professional Mobile Radio), to support communication in critical situations, where participants listen and talk on the same radio frequency.

These analogue systems have been characterized by:

- The ability of many professionals talking on the same frequency
- Push-to-talk (sub-second delay from pushing a talk button to talking).
- The ability for radios to work without any infrastructure (DMO: Direct Mode Operation).
- Radios designed for water and heat-resistance to be used in extreme situations.

Technological developments has made it possible to design digital infrastructures that have the same characteristics as analogue radio systems, while adding a number of possibilities because it is digital. The digital infrastructures for public safety communications, such as TETRA and TetraPol, provide a number of features that improve them over old analogue ones:

- Talk groups replaces shared radio frequencies and offers a much more flexible approach to group communications across geographical and organizational boundaries.
- Encryption, to allow communication, which cannot be eavesdropped.
- Possibility of scaling to support all of public safety and to support communication across forces.
- One-to-one calls to work like a PSTN or GSM phone.
- Transfer of data, including GPS-positions, which enables a geographic overview of resources deployed.

The communication needs and available communication technologies have evolved over time and have formed the requirements for infrastructures for public safety communications.

These requirements are driving the establishment of dedicated regional or national Wireless Network Infrastructures for command & control in most countries. In the following we shall refer to these as CCWNI (Command & Control Wireless Network Infrastructure).

3.1. Requirements for national public safety networks

In a number of European countries, Investments have been made in national CCWNI's.

Gartner has captured the requirements that were included in the political decision to invest in a dedicated Command & Control Radio Wireless Infrastructure (CCWNI) in Norway and in Denmark, Sweden and Germany. The comparison of these would indicate whether the Norwegian decision to procure a TETRA network is based on exceptional requirements rather than comparable requirements.

3.1.1. Norway:

The decision to start initial build out of Nødnett was based on the following promised benefits from a shared national public safety radio infrastructure[1].

- Secure against eavesdropping
- Shared communication groups for the police, fire and health services
- Improved indoor coverage
- Improved voice quality, background noise is removed
- Possibility of transmitting data
- Two-way contact with part-time crews in case of fire
- Transmission of ECG / remote observation
- Complete overview of vehicles and crews

Based on Stortingspropositionen and other relevant documents Gartner has captured the overall requirements for Nødnett in the following matrix:

Requirement name	Description
Same radio system in all of public safety	Common national radio system
Encryption capabilities	Digital radio network (possibility to communicate without eavesdropping – Police, encrypt sensitive health data and encrypt firemen's communication). End to end encryption required.
VPN capability	Virtual Private Networks for organisations using it.
Nationwide coverage	Nationwide coverage
Voice quality	Good voice quality in noisy areas
Support Group calls	Group calls, individual calls and data transmissions. Group calls across VPN's and

[1] Proposition No. 1 to the Storting – Supplement No. 3 (2004–2005)

Requirement name	Description
	geography
Support individual calls	Yes
Support data transmissions	The system can transmit data as text messages, pictures, map sectors, ECGs and database look-ups.
Paging	Include a pager solution
Traffic prioritizations and alarm calls	Alarm calls and prioritized traffic
DMO support	Possibility of DMO. Direct Mode Operations enabling direct communication between units within range (when no base station is available)
Integration with other public safety networks	Integration/compatibility with public safety networks in adjacent countries to support cross border operations
Available Frequency band	A spectrum should be available for the network.
High Availability	The infrastructure should be available in extreme circumstances including power outages and incidents were e.g. public telecom nets does not work.
Integration with PSTN's	The ability to call from/to phones in the public fixed and mobile networks

This list of technical requirements from the Norwegian procurement has formed the basis of a comparison with Sweden, Denmark, and Germany. They have been selected because they are recent procurements in neighbouring countries and because material was available to document the overall requirements used in the political decisions.

3.1.2. Sweden[1]

When the Swedish government decided to procure a CCWNI in 2003 (to become known as RAKEL), the following of the Norwegian requirements were involved in the decision.

Requirement name	Required in decision to procure
Same radio system in all of public safety	Yes - Common national radio system used for public all public safety
Encryption capabilities	Yes – no additional end-to-end encryption required
VPN capability	No – although system should support flexible cooperation and co-existence.
Nationwide coverage	Yes
Voice quality	Yes - Good voice quality in noisy areas

[1] Section 9.2.2 in Report "Trygga medborgera – säker kommunikation"

Requirement name	Required in decision to procure
Support Group calls	Yes - Support dynamic groups
Support individual calls	No
Support data transmissions	Yes
Paging	No
Traffic prioritizations and alarm calls	Yes
DMO support	Yes
Integration with other public safety networks	Yes
Available Frequency band	Yes
High Availability	Yes
Integration with PSTN's	Yes

3.1.3. Denmark

In Denmark, the decision to procure a CCWNI was taken in early 2006. The following Norwegian requirements were used as a basis for the decision:

Requirement name	Required in decision to procure
Same radio system in all of public safety	Yes (incl. Police, Ambulance, Fire)
Encryption capabilities	Yes – not end-to-end encryption required
VPN capability	Yes
Nationwide coverage	Yes
Voice quality	Yes
Support Group calls	Yes
Support individual calls	Yes
Support data transmissions	Yes
Paging	No
Traffic prioritizations and alarm calls	Yes
DMO support	Yes
Integration with other public safety networks	Yes
Available Frequency band	Yes
High Availability	Yes
Integration with PSTN's	Yes

3.1.4. Germany[1]

The decision to build out a CCWNI in Germany has been taken in a number of steps, but the agreement between the different Bundesländer to cooperate on building out a national CCWNI was taken in July 2007. The German network, referred to as Digitalfunk BOS, was decided based on the following of the Norwegian requirements.

Requirement name	Required in decision to procure
Same radio system in all of public safety	Yes
Encryption capabilities	Yes
VPN capability	Yes
Nationwide coverage	Yes
Voice quality	Yes
Support Group calls	Yes – group
Support individual calls	Yes
Support data transmissions	Yes
Paging	No
Traffic prioritizations and alarm calls	Yes
DMO support	Yes
Integration with other public safety networks	Yes
Available Frequency band	Efficient use of available frequencies
High Availability	Yes
Integration with PSTN's	Yes

3.1.5. Requirements compared

The comparison of the requirement matrices for the four countries shows overall a very close correlation between the requirements. Norway has two overall requirements that have not been part of requirements in the other countries. These are requirements regarding paging and end-to.end encryption.

Paging

By paging is meant that the public safety infrastructure is used for paging firemen (and potentially other people on duty remotely).

In a number of European countries, where new CCWNI's have been and are being established, the question of whether to use the network for paging has come up. In Norway the decision was made to use the CCWNI for paging. In other European countries investments have been made in separate paging infrastructures or the existing paging systems have been reused.

[1] Source BDBOS.bund.de, and "Verwaltungsabkommen über die zusammenarbeit zwischen Bund und Länder beim aufbau und betrieb eines bundesweit einheitlichen digitalen Sprech-. Und Datenfunksystem für alle Behörden und Organisationen mit sicherheitsaufgaben in der Bundesrepunlik Deutschland" (july 2007).

The typical reason for deciding not to use the CCWNI has been the lack of available pagers to use on the CCWNI infrastructure. TETRA has been chosen in all recent investments in European national CCWNI's and there are for the time being no pagers available on the market. In TETRA ordinary handheld terminals can be used, but have been discarded both because of price and limited battery life.

This issue of whether to use the infrastructure for paging is however not significant in terms of choosing the right technology for the infrastructure. It is not a differentiating factor between technologies.

End-to-end encryption

Communications on CCWNI's use different means of encryption. The most common method used is over-the-air encryption eventually supplemented by encryption of the communication on the backbone. However, encryption from terminal to terminal is required from some organizations like intelligence services to allow for classified communication (commonly referred to as end-to-end encryption). Achieving end-to-end encryption is generally an issue of functionality in terminals and not an issue for the underlying CCWNI technology. End-to-end encryption in TETRA is achieved by procuring special terminals with this capability.

In sum

The requirements that are determining choice of technology is generally the combination of group calls, short call-setup times, traffic prioritization, high availability, and of course the availability of a frequency spectrum.

Overall, the requirements underlying the decision to procure Nødnett are therefore very well aligned with the requirements in the comparison Gartner has undertaken. From anecdotal evidence this is the case in most other countries as well.

3.2. Broadband radio networks for public safety

As mentioned above, public safety organizations (especially Ambulances, but also Police forces) are looking for supplementing the CCWNI with 3G or other technologies with broadband data capacity.

For this purpose, public 3G networks are being used, except in one case known to Gartner in New York City. Here, a city-wide wireless broadband network based on TD-CDMA, is being rolled out. The rollout is planned to be complete by the end of 2008. The network is utilizing 10 MHz in the 2,5 GHz band.

This is a dedicated network built to support a number of applications, not just public safety, but also other public services. Applications utilizing the network include: automated vehicle location, automated water-meter-reading, synchronization of traffic signals, and footage from incidents and emergencies. The New York Fire Department will utilize the network for GIS-data, photos, videos, and maps.

Gartner expects, however that most public safety organizations with broadband requirements will decide to utilize public networks because of the significantly lower prize.

3.3. A survey of essential requirements

As part of the work on this report, Gartner has performed a small survey among a number of key decision makers and experts, working with public safety radio networks [1]. Five respondents were decision makers from Europe and one from USA.

The participants were asked to answer the following question: if you were to invest in an infrastructure for operational public safety communications today (a CCWNI), what would be the essential requirements?

The following requirements were agreed by all (n=6) to be essential:

Requirement name	Description
Encryption capabilities	Communication is over-the-air encrypted
VPN capability	The infrastructure supports more individual organisations communicating securely and inaccessible from other organisations
Good Voice quality	Provides good voice quality in noisy surroundings.
Support Group calls	Supports geographically and organisationally dispersed group calls.
High Availability	The infrastructure has high availability in emergency situations
Integration with PSTN's	The infrastructure can integrate with public telephone networks.

The following requirements were agreed by 4 or 5 of the respondents:

Requirement name	Description
Same radio system across all of public safety	Radio infrastructure will be shared across police, fire, ambulance, and other
Nationwide coverage	The radio infrastructure provides countrywide overage and interoperability
Support individual calls	Supports one-to-one calls
Support data transmissions	Radio infrastructure supports packet-switched data.
Paging	Radio infrastructure can be used to call out fire personnel.
Traffic prioritizations and alarm calls	Traffic can be prioritized in overload situations.
DMO support	The end-user devices support direct communication without infrastructure.

[1] The number of answers was 6, so quantifying the statistical significance is not relevant. It, however gives clear indications of the direction of requirements, were they to invest in a public safety radio infrastructure *today*.

Requirement name	Description
Integration with other public safety networks	The radio infrastructure can be integrated with other infrastructures

The following requirement was only rated as essential by one decision maker.

Requirement name	Description
High-bandwith data	The infrastructure supports high-bandwidth data. (as delivered by 3G)

The underlying reasons for decision makers not to rate this as an essential requirement is probably a mixture of two. Firstly, most public safety organizations have not started demanding, building and procuring the applications requiring high-bandwith data. Secondly, as we shall see in the evaluation of technologies, there are no technologies available that can both meet the other essential requirements for a CCWNI and deliver high-bandwith data.

Based on the survey a list of essential requirements for a public safety radio infrastructure should therefore include the following:

Table 1 List of essential requirements for a CCWNI

Requirement name	Description
Same radio system across all of public safety	Radio infrastructure will be shared across police, fire, ambulance, and other
Encryption capabilities	Communication is over-the-air encrypted
VPN capability	The infrastructure supports more individual organisations communicating securely and inaccessible from other organisations
Nationwide coverage	The radio infrastructure provides countrywide overage and interoperability
Good Voice quality	Provides good voice quality in noisy surroundings.
Support Group calls	Supports geographically and organisationally dispersed group calls.
Support individual calls	Supports one-to-one calls
Support data transmissions	Radio infrastructure supports packet-switched data.
Paging	Radio infrastructure can be used to call out fire personnel.
Traffic prioritizations and alarm calls	Traffic can be prioritized in overload situations.
DMO support	The end-user devices supports direct communication without infrastructure.
Integration with other public safety networks	The radio infrastructure can be integrated with other infrastructures including other countries
High Availability	The infrastructure has high availability in emergency situations

Requirement name	Description
Integration with PSTN's	The infrastructure can integrate with public telephone networks.
Short call setup times[1]	The time should be less than 500 ms.
End-to-end encryption[2]	Communication is encrypted from terminal to terminal.

This survey shows that decision makers, were they to procure a CCWNI today, would use the above list of essential requirements. Again, compared to the Norwegian requirements used to procure Nødnett, the requirements are in line. As can be observed, the above list of essential requirements even includes end-to-end encryption and paging. These were the two requirements not used in the Swedish, Danish or German procurements.

3.4. Essential requirements for a CCWNI

Gartner has compared the Norwegian requirements in two ways. Firstly, they were compared with recent procurements in neighbouring countries, secondly with a survey of decision makers and experts working with CCWNI's[3].

Both comparisons show that the requirements for Nødnett are in line with what is required elsewhere. Even if compared to the survey response from experts from USA, where different technologies are used than in Europe, the requirements are in line.

The essential requirements listed above in Table 1 will be used in section 4 to evaluate existing and emerging technologies for building wireless infrastructures, of which a CCWNI should be considered a special case.

Gartner observes, however that communication requirements are likely to evolve over the coming years.

3.5. On evolving communication requirements in public safety

Public safety organizations needs for communication is bound to develop. This happens both as a result of technology developments in society in general and because public safety organizations in many countries are provided with extra resources for developing and procuring new technologies to meet new threats such as terrorist attacks. The trends that are affecting the need for communications solutions include the following:

- Data-intensive solutions in healthcare: where communication takes place between ambulance and hospital in order to improve treatment on the scene of the incident or on the way to the hospital.
- Mobile offices in Police: Police will have access to databases and case management systems, so they can stay mobile a larger percentage of their working time.
- The use of images, video and other footage in investigations and pursuits.

[1] This requirement was not on the original list, but was suggested by half of the respondents.

[2] This requirement was not on the original list, but was suggested by half of the respondents. The organizations requiring end-to-end encryption are users with special security needs such as intelligence services.

[3] None of the survey respondents were from Sweden, Denmark or Germany.

- The use of public GSM phones for communication in police, fire, and healthcare. These are used because of their simplicity and flexibility – everybody has a GSM phone.

In sum, public safety organisations require increasingly high-bandwidth data solutions and flexible communications with people outside the organisation. And still, the public safety organisations have a need for a communications technology, which supports group calling, quick call-setup times and guaranteed availability in critical situations.

The question is then, whether all need for communication services could be met by one network infrastructure. The answer to that question is: no. The reasons are:

GSM phones are there as a fact of life and is already being used by public safety personnel. Public safety organisations might as well utilize this and see the GSM phone as a backup alternative in situations where the operational network does not have coverage, etc.

There is no technology in place with both the essential characteristics of a public safety radio communications network (group calls, fast call-setup times, etc.) and the bandwidth available to support the needs in the foreseeable future for transferring images, videos, patient records, etc.

Therefore, the most likely scenario for supporting the communication needs of public safety organisations such as police, fire, and ambulance is:

1. A dedicated public safety network infrastructure primarily for operational communication in incidents – a dedicated command and control network with some limited data capabilities. Referred to as CCWNI (Command & Control Wireless Network Infrastructure).
2. GSM-phones will be used, especially for communications across forces and with organisations outside of public safety as a complement when available.
3. High-bandwidth data connections will be delivered by either public services, such as 3G (UMTS/CDMA2000), Wi-Max or WLAN or by a dedicated network (as seen in New York City) as an overlay service to the command and control network.

History has shown over and over again that a public network can not be dependent on for mission critical communications by public safety organizations. One such example was during the July 7th bombings in London where the public GSM networks collapsed due to overload despite that they were set up to give priority to pre-authorized government subscriptions.

Although it will not serve all communication need for public safety in the future, the essential requirements for a CCWNI should still form the basis for an evaluation of technologies for building such an infrastructure, because it supports the communication requirements that are unique to public safety.

4. Technology landscape for public safety networks

As noted earlier, public safety is undergoing big changes internationally, driven by the evolution of technology in society in general and driven by the significant increase in spending on public safety since 9/11 and other terrorist attacks.

In Europe most countries either have or are in the process of rolling out a national dedicated CCWNI to support the operational communication of public safety organisations.

In USA dedicated networks are being rolled out state wide (E.g. New York State) and in large cities and in Asia regional networks are also being rolled out.

The public authorities in USA are in the process of auctioning frequency spectrums in the 700 MHz band for a nationwide public safety network. As both experiences from Denmark show and experts in USA note, building out a national CCWNI based on auctioning the frequency spectrum is however very unlikely to work.

Also, as public safety technologies evolve there is an increasing need for high-bandwidth solutions. In Europe this trend is most obvious with ambulance service, where there is an explicit demand for sending data between incidents/ambulances and patient record systems and other systems, typically located in hospital data centres.

In Denmark, Norway, France, UK and other countries, ambulances are currently using GPRS/EDGE/3G on public networks to support data communications as an overlay to the public safety network.

In addition to using the essential requirements to evaluate technologies, other aspects are highly relevant as well. These aspects have to do with the availability and maturity of technologies and markets for these technologies.

There are three primary aspects of the technology that should be considered of which two are crucial for the selection of technology:

Firstly, there should be a market from which it is possible to procure infrastructure technology to build a CCWNI. This means that vendors should exist that produce and market these technologies.

Secondly, there should be a market for terminals that will work on the infrastructure. As noted earlier, the special communication requirements in public safety will require terminals that can be operated easily in extreme situations.

Thirdly, a CCWNI should be integrated with control rooms, from which resources can be dispatched and controlled. The integration of infrastructures with control rooms is, however not a deciding factors, because it only requires an API (Application Programming Interface) in the infrastructure.

As a consideration related to the risk involved in investing in a technology for a CCWNI, the existence of other infrastructures in use for public safety should be added as a criteria. Being the only or first to use a technology for a CCWNI involves a significant risk, which is generally avoided for mission critical systems.

Relevant to evaluating the cost of infrastructures is also the question of frequency spectrum used. Radio planning is the art and science of determining where to put up infrastructure base stations to provide radio coverage for terminals and is a complex undertaking involving both capacity and coverage issues. However, in general, technologies that operate in higher frequency bands provides a smaller coverage area per base station than technologies operating in lower frequency bands. This means that technologies operating in higher frequency bands require more base stations to cover the same area than does one operating in a lower.

Because, the number of base stations is a major cost driver for all Wireless Network Infrastructures, including CCWNI's, the frequency spectrum used could also turn out to be a decisive factor. It is however only of relevance if the technology meets the essential requirements and has a market for both terminals and infrastructure.

4.1. Public networks or private network for public safety

The possibility of utilizing existing public network infrastructures such as GSM/GPRS/EDGE and 3G has been discussed as a possibility of solving the needs for CCWNI. However, the conclusions have always been that public networks would need significant architectural changes to accommodate the requirements for availability in critical situations. Also public networks built on GSM/GPRS and 3G are built to support one-to-one calls and needs modifications to accommodate the need for supporting group calls.

In short, there are no examples known to Gartner, where countries, regions or cities are supporting the needs for operational public safety communications (Police, Fire, and Ambulance) based exclusively on a public network.

There are some local examples of organizations with public safety work, using public networks. In Louisiana, Rivada Networks acts as a virtual mobile operator for the Louisiana[1] army National Guard on a Sprint public network and provides an additional mobile CDMA infrastructure to supplement requirements during large incidents. The number of users is around 1000. Also, Ericsson markets QuicLink, a GSM/3G network, which can be transported on a trailer to act as a temporary infrastructure in large incidents.

However, none of these solutions are being used as the primary means of operational communication (command & control) in public safety operations. Therefore the focus of the following evaluation of possible technologies will be on dedicated infrastructures for public safety – or private networks.

4.2. Existing technologies for wireless infrastructures.

Wireless wide area network infrastructures are dominated by two families of technology standards and some competing standards focusing on wireless data transmissions.

GSM family:

GSM is used in 900 and 1800 MHz in Europe, evolving with data capabilities GPRS/EDGE (often referred to as 2G and 2.5G). All European operators has added 3G based on WCDMA in 2100 MHz. 3G has evolved with HSPA (High Speed Packet Access) increasing initially downlink speed and later uplink speed into multiple Mbps. The GSM family will over time evolve to HSPA+ and/or LTE and LTE-A.

CDMA family:

CDMA is used predominantly in North America and a couple of countries in Asia/Pacific. It has a similar evolution with CDMA 2000 1.xRTT, EV-DO rev 0 and rev A and an evolution path to UMB.

Figure 1 illustrates the likely development of the two technology families.

[1] http://urgentcomm.com/mobile_voice/news/rivada_contract_louisiana_121907/index.html

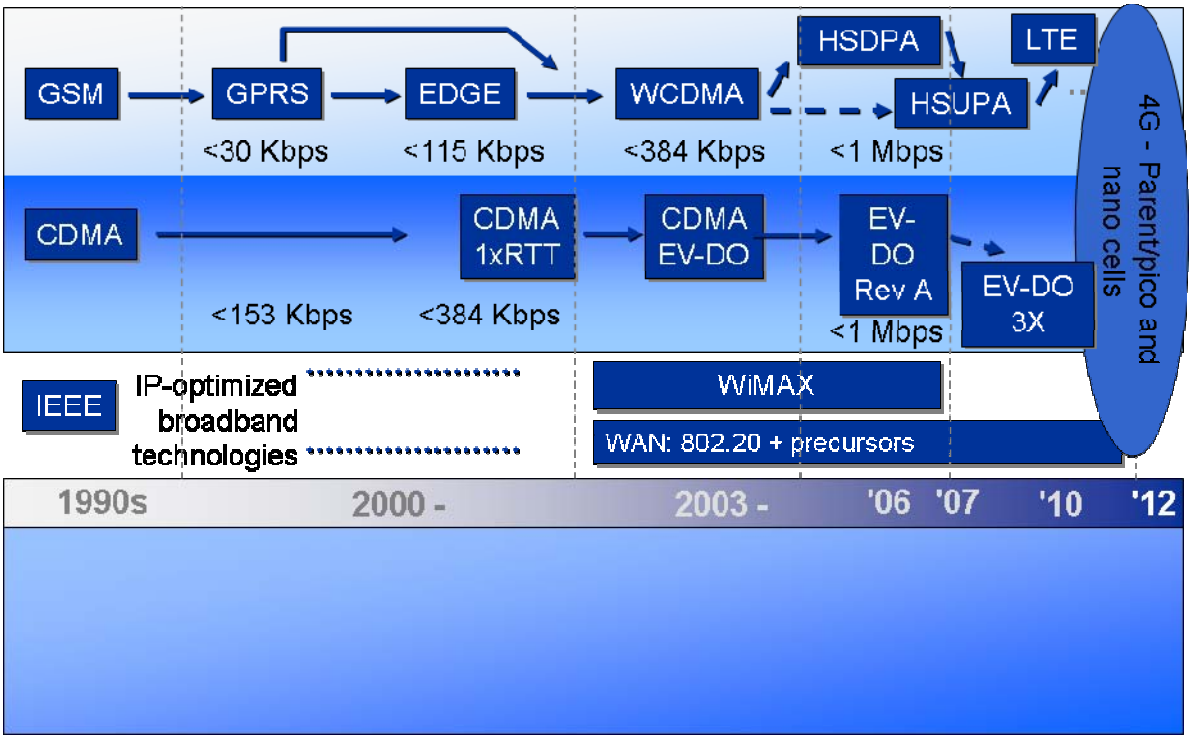

Figure 1: Evolution timeline for GSM and CDMA families and WiMAX.

In addition to the two technology families there are some competing Wireless Wide Area Networking standards predominantly focused on transferring data:

- 802.16 – WiMAX – started as a fixed standard ratified as 802.16-2004 f k a 16d and then a mobile standard, 802.16e-2005, f k a 802.16e.
- 802.20 – Flarion/OFDM – promoted by Siemens in the 450 Mhz band. Used in Finland and a couple of CEE countries.
- UMTS-TDD, mostly IP Wireless implementations, e g Czech Republic, Slovakia and some other countries.

In the following these technologies will be evaluated separately.

4.2.1. GSM with GPRS/EDGE

GSM is the most adopted technology standard for mobile communications. With GPRS/EDGE it also provides data communication.

Due to the availability of public GSM infrastructures in all European countries, a number of evaluations of the use of public GSM networks have been performed for the use of GSM for CCWNI. None of them has, however meant that any CCWNI's have been built on GSM.

Gartner expects that investments in mobile infrastructures in GSM/GPRS/EDGE will start declining in 2009 and shift to 3G technologies. Operators will however continue to "backfill" rural areas with GSM/GPRS/EDGE as a cost effective way to improve coverage.

Requirement name	GSM Evaluation
Same radio system across all of public safety	Unproven
Encryption capabilities	Yes, however technology to decrypt is readily available

Requirement name	GSM Evaluation
VPN capability	Yes with some operators, requires additional investments
Nationwide coverage	Yes
Good Voice quality	Yes
Support Group calls	Unproven
Support individual calls	Yes
Support data transmissions	Yes (with GPRS/EDGE)
Paging	Yes
Traffic prioritizations and alarm calls	Unproven
DMO support	Yes, but not sufficient for public safety users
Integration with other public safety networks	Unproven
High Availability	Yes, for central nodes but class b and c nodes typically have only 4-12 hours of UPS available
Integration with PSTN's	Yes
Short call setup times	No
End-to-end encryption	No

Available market for infrastructure: Yes, but not for public safety uses.

Available market for terminals: Yes, but not for public safety uses.

Infrastructures in operation within public safety: Yes but not for operational public safety.

It would be theoretically possible to build a dedicated network infrastructure based on GSM. This would, however require a very large investment. Also it would require the development of special terminals to operate in the 380 – 400 MHZ spectrum available for public safety.

In sum, GSM is not an interesting option for a CCWNI. GSM can and is being used as a supplement when it is available, mainly because of the wide availability of GSM phones – everybody has one.

4.2.2. WCDMA (evt. with HSDPA)

Wideband code division multiple access (WCDMA) is a Universal Mobile Telecommunications System (UMTS) standard for 3G digital mobile networks, using code division multiple access (CDMA) technology. It is the evolutionary path to UMTS for Global System for Mobile Communications (GSM) and Enhanced Data Rates for Global Evolution (EDGE), and offers increased voice capacity and theoretical peak data speed of up to 2 Mbps. The 3GPP task group continues to work on the development of WCDMA toward 4G, and has defined a series of evolutionary steps, including High-Speed Downlink Packet

Access (HSDPA), High-Speed Uplink Packet Access (HSUPA) and Long-Term Evolution (LTE), which are integral parts of the WCDMA evolution.

Adoption by end users is slower than anticipated. Customer uptake is still very limited, despite extensive network rollout worldwide. Adoption by consumers and enterprises is driven more by handset subsidy and service pricing than by WCDMA and UMTS capabilities. It is very widespread in networks, despite relatively low subscriber usage, with 155 commercial WCDMA networks in 58 countries. There are regional differences and, in some markets, adoption and usage are higher.

For example, all four mobile operators in Australia have deployed WCDMA. One of these, Hutchison, has been WCDMA-only for three years, and Vodafone and Telstra aim to convert all of their GSM subscribers to WCDMA by the end of 2008. Three of these networks already offer HSDPA Phase II, and Telstra will offer Phase III by the end of this year.

Telenor and Netcom both have WCDMA infrastructures rolled out in Norway. Telenor and Netcom are currently rolling out HSDPA (High-Speed Downlink Packet Access) to increase the downlink data speed on the existing WCDMA network.

The use of WCDMA is only widespread for public mobile phone infrastructures in countries where GSM has been used. There are no known examples of WCDMA infrastructures used for private infrastructures.

There is a mature market for both infrastructures and end-user devices (phones, smart-phones, pda's, etc., data-access cards), but there is not a market for terminals directed at the use for public safety personnel.

In order for WCDMA to support the operational needs of public safety personnel, capabilities such as group calls, individual calls, prioritization and security, would have to be built on top of e.g. TCP/IP using WCDMA as a data channel. This would again require special terminals built for public safety use. If Norway were to rely on WCDMA, it would therefore have to bare all risks and costs associated with developing these terminals.

Gartner does not expect WCDMA adoption for CCWNI use, and thus there will be no one with whom to share the risk and costs.

Requirement name	WCDMA Evaluation
Same radio system across all of public safety	Unproven
Encryption capabilities	Yes
VPN capability	Needs proprietary development
Nationwide coverage	Yes
Good Voice quality	Yes
Support Group calls	Must be designed as e.g. voice over IP solution
Support individual calls	Yes
Support data transmissions	Yes
Paging	Yes

Requirement name	WCDMA Evaluation
Traffic prioritizations and alarm calls	Needs proprietary development
DMO support	Needs proprietary development
Integration with other public safety networks	Unproven
High Availability	Yes
Integration with PSTN's	Yes
Short call setup times	Unproven
End-to-end encryption	Needs proprietary development

Available market for infrastructure technologies: Yes

Available market for terminals: Yes, not for public safety purposes

Infrastructures in operation within public safety: No

No known uses of the technology within public safety as primary or only network. Used in some countries as a complementary data overlay for applications such as transferring journal and patient data back and forth between ambulances and acute-care units.

4.2.3. Wi-MAX (802.16)

WiMAX 802.16e-2005 is a mobile version of the IEEE 802.16-2004 standard. It supports time division duplex (TDD) frequencies, most commonly used in 2.3 to 2.5 GHz and 3.3 to 3.5 GHz, and is therefore of interest to service providers who hold or can get hold of this spectrum. WiMAX 802-16e-2005 is coming to market to support mobile, metro area and broadband wireless capabilities.

WiMAX 802.16e-2005 gains attention, especially in emerging countries, as a last-mile access technology to provide Internet services. First devices were certified for 2.3 GHz in April 2008. We expect further devices supporting other frequencies to become certified in 2008 and beyond. We also expect Intel to launch a single Wi-Fi/WiMAX mobile chipset in 2008, and its deployment in laptops or other mobile Internet devices. Most WiMAX mobile networks will be deployed for rural coverage, beginning with coverage in a defined area, such as city networks. A few nationwide deployments have been announced, the latest by KDDI Corporation in Japan, while Sprint's launch in the U.S. has already been delayed by six to nine months. User devices will still be limited in availability, and the focus in data, versus combining voice and data, will limit market appeal.

WiMAX network availability is still limited. Consider WiMAX as a broadband access service, especially if no alternative infrastructure is commercial. It can also be considered as an alternative for Wi-Fi or Pico cells at campus for enterprise wireless data connections, if private licenses are available.

Gartner characterize 802.16e-2005 WiMAX is a mobile technology which will be used for defined areas, such as digital subscriber line (DSL) fill-in in rural areas, rather than as a nationwide system for voice and data. It will be competitive, with high-speed third generation (3G) cellular services when it is launched.

No planned networks with complete coverage in Norway known to Gartner. We expect some regional networks to start up based on the local competitive situation.

Gartner predicts the following for the commercial use of WiMAX in public networks:

- Mobile WiMAX will be a component of service providers' access technology portfolios. It will be a part of the service providers' arsenal in delivering seamless services (independent of technology platforms and devices) to end users.
- By 2016, the basis of competition is expected to shift to applications, content and tangible value delivered to end users. Competition will not be couched in terms of mobile WiMAX versus cellular or any other access technologies.
- Complementarities (for example, those of end user devices [variety, functionality and price] and applications) will play a pivotal role in determining the service providers' success with mobile WiMAX.
- New entrants using mobile WiMAX in conjunction with a "low retail price" go-to-market strategy alone will encounter difficulties. Market incumbents will react aggressively, and they typically have the ability to bundle service offerings and withstand prolonged price wars.

There are no indications that mobile operators will be able to present a business case for providing WiMAX coverage to fit the needs of public safety.

There is an emerging market for WiMAX enabled phones, but major investments in WiMAX infrastructures have not started.

Requirement name	WiMAX Evaluation
Same radio system across all of public safety	Yes
Encryption capabilities	Needs proprietary development
VPN capability	Needs proprietary development
Nationwide coverage	Possible but very unlikely with a public network
Good Voice quality	Yes
Support Group calls	Must be designed as e.g. voice over IP solution
Support individual calls	Yes
Support data transmissions	Yes
Paging	Yes
Traffic prioritizations and alarm calls	Depends on provider
DMO support	No
Integration with other public safety networks	Unproven
High Availability	Possible
Integration with PSTN’s	Yes

Requirement name	WiMAX Evaluation
Short call setup times	Unproven
End-to-end encryption	Needs proprietary development

Available market for infrastructure: Yes

Available market for terminals: Yes, but immature and not for public safety

Infrastructures in operation within public safety: No.

4.2.4. TD-CDMA

TD-CDMA and its Chinese cousin, TD-SCDMA, are 3GPP-approved time division duplexing (TDD) air interfaces defined by the UMTS 3G cellular mobile phone standard and mainly used to provide Internet access. In TDD, the same spectrum is shared for the uplink and the downlink via time division. TD-CDMA uses 5MHz channels, each divided into 10 milliseconds (ms) frames and each containing 15 time slots (1,500 per second). CDMA is used in each time slot to support multiple users. TD-SCDMA uses 1.6MHz channels. In much of Europe and Asia, a specific UMTS-TDD spectrum of 1,900MHz to 1,920MHz and 2,010MHz to 2,025MHz have been set aside, and operators often were obliged to buy a TDD spectrum along with the UMTS-FDD paired-frequency spectrum they needed for 3G voice. A band of 2,500MHz to 2,690MHz has been used for TDD in some countries (for example, in the U.S.), and 3.5GHz in others (for example, in the U.K. and New Zealand). Although TD-SCDMA still is undergoing trials in China, TD-CDMA has been deployed in more than a dozen commercial wireless broadband and public-safety networks globally by IPWireless (NextWave).

The future of this technology is uncertain and it does not provide any advantages over the mainstream 3G technologies. It should therefore not be considered for public safety purposes either. In addition to the risks involved in developing e.g. the WCDMA infrastructure to support the needs of public safety, one would with TD-SCDMA run the risk of basing it on a technology dead-end.

4.2.5. GSM-R

GSM-R (GSM for Railways) is an international wireless standard for railway communications. It is based on GSM but has entered its own evolution path. It is being used/deployed by most European national railway systems but has found very little use outside railway operators (see Figure 2).

GSM-R is derived from GSM and the technology therefore has many similarities to GSM.

In terms of cost, providing nationwide coverage with GSM-R would constitute a large investment. GSM-R in Europe has allocated frequencies in the 800 – 900 MHZ band, and although some coverage exist around the railways in Norway, providing coverage nationwide to support public safety would be very costly.

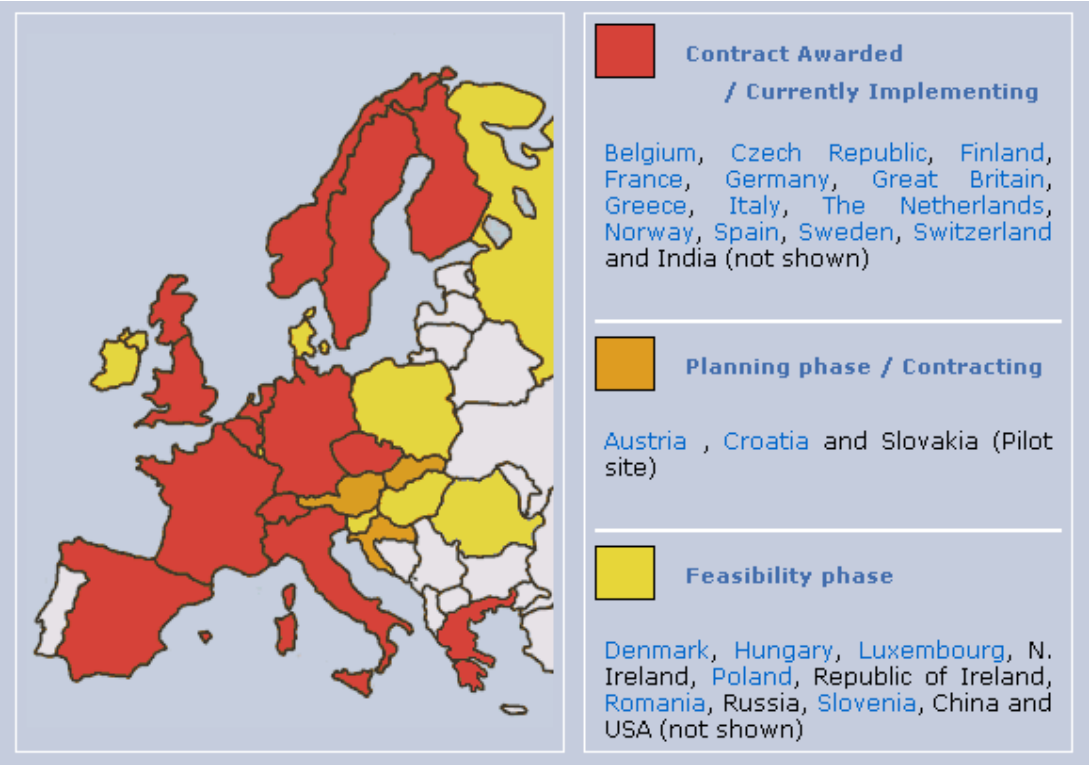

Figure 2: GSM-R rollout status as of May 2006 (Source: gsm-r.uic.asso.fr)

Requirement name	GSM-R Evaluation
Same radio system across all of public safety	Unproven
Encryption capabilities	Needs proprietary development
VPN capability	Needs proprietary development
Nationwide coverage	Possible but very costly
Good Voice quality	Yes
Support Group calls	Yes
Support individual calls	Yes
Support data transmissions	Yes
Paging	Unproven
Traffic prioritizations and alarm calls	Yes
DMO support	No
Integration with other public safety networks	Unproven

Requirement name	GSM-R Evaluation
High Availability	Possible
Integration with PSTN's	Yes
Short call setup times	Unproven
End-to-end encryption	Needs proprietary development

Available market for infrastructure: Yes

Available market for terminals: Yes, but not for public safety needs

Infrastructures in operation within public safety: No.

GSM-R meets more of the essential requirements for public safety than does the technologies used for public infrastructure. The major obstacle to using GSM-R as a technology is the cost associated with building nationwide coverage and the unavailability of terminals for public safety needs. No vendors have, to the knowledge of Gartner, made a bid for a nationwide or regional CCWNI in Europe. Mostly likely because it would be financially unattractive, even when reusing base stations already set up for railway use.

4.3. Emerging technologies for mobile infrastructures.

4.3.1. Voice over IP solutions using WCDMA/CDMA2000/WiMAX

It has been suggested to model traffic prioritization, group calls and shot call-setup times requirements for public safety using Voice over IP on top of a 3G/broadband technology. This idea would require an IP-based PBX and is an idea, which has not been proven to work. Exactly how to provide short call-setup times and efficient group calls is not proven.

Available market for infrastructure: No

Available market for terminals: No

Infrastructures in operation within public safety: No.

4.3.2. Long-Term Evolution-A (LTE-A)

LTE-A is supposed to be the first fully compliant version to the International Telecommunication Union (ITU)-T specification for 4G systems. The targeted peak rate for downlink (DL) is 1 Gbps and for uplink (UL) greater than 500 Mbps. This should be achieved with scalable usage of up to 100 MHz spectrum. LTE-A should support various cell types including Pico and Femto to improve uplink speeds as well as relay technologies to improve coverage. Furthermore, LTE-A should be backward compatible to LTE, Rel. 8. The scoping phase of LTE-A will go along with a further ITU-T specification of 4G.

LTE-A is in scoping phase in 2008 and the standardization might be finished at the earliest in 2011. Therefore, certified equipment for LTE-A can be expected 18 to 24 months after standardization which means 2013. After 2013, commercial roll-outs and upgrades of LTE systems will start and mass market deployment will happen during the next five years, around 2018.

With this expected timeline, this technology is not relevant to consider for public safety infrastructures in the near term.

4.3.3. WCDMA upgrades (with HSUPA and LTE)

High-Speed Uplink Packet Access (HSUPA) is a standard for fast data uploads over Universal Mobile Telecommunications System (UMTS) networks. It forms part of the Release 6 specifications from the Third Generation Partnership Project (3GPP), and is integral to the 3G cellular technology known as wideband code division multiple access (WCDMA). HSUPA complements High-Speed Downlink Packet Access (HSDPA) by increasing upstream data bit rates on 3G networks. At present, it raises them to 1.45 Mbps (peak), but the technology will develop to support a theoretical maximum of 5.8 Mbps at cell level. HSUPA also improves latency, which will typically fall to 80 milliseconds (ms). In addition, the technology shortens round-trip times to approximately 70 ms. The aim is for HSUPA and HSDPA to deliver symmetrical uplink and downlink data rates, so that 3G networks can support applications such as videoconferencing. The two technologies share many of the same techniques, such as adaptive modulation and hybrid automatic repeat request.

At least 34 carriers have launched HSUPA services, and 66 HSUPA-capable user devices have been launched, according to an April 2008 survey by the Global Mobile Suppliers Association.

Long-Term Evolution (LTE) is a Third-Generation Partnership Project (3GPP) project to define the requirements and basic framework for the wideband code division multiple access (WCDMA) mobile radio access network beyond third generation (3G). It is also known as Release 8, probably the last step before fourth generation (4G). The core specifications for Release 8 were completed by end of 2007, with some early commercial deployments beginning toward the middle of 2010. LTE includes objectives such as 100-Mbps download and 50-Mbps upload peak data rates in 20MHz of spectrum, full mobility to speeds of up to 500 kilometers per hour, support for 3G network overlay and hand-overs between 3G and LTE. We expect LTE to compete with 802.16e if at all, but not with 802.16m. Beyond LTE, we expect competition between LTE-A and 802.16m. Gartner estimates that Japan, South Korea and the United States will be leading in terms of early deployments in 2009 and 2010.

WCDMA with HSUPA or LTE does not constitute interesting options for public safety for the present time. Mainstream adoption of LTE is expected to begin around 2012 and the technology will at that time have the same issues with meeting public safety requirements as does WCDMA today.

4.3.4. Mesh Networks: Sensor

Sensor networks are ad hoc networks formed by dynamic meshes of peer nodes, each of which includes simple networking, computing and sensing capabilities. Some implementations offer low-power operation and multiyear battery life.

Position and Adoption Speed Justification: Small-to-midsize implementations (that is, tens to hundreds of nodes) are being deployed using technology from several vendors. This technology is being adopted by Type A (aggressive technology adopter) companies. The market is commercially and technologically fragmented, and topics such as middleware and power-efficient routing are still areas of active academic research. Proprietary and more-standard technologies are used for radio frequency bearers and the software stack, depending on the vendor. Some companies have adopted ZigBee as a standard radio frequency bearer; some use proprietary systems; and some have formed industry alliances around technologies for specific applications (for example, Z-Wave for home automation). It's likely that a new ultra-low-power Bluetooth standard (arriving in 2009) also will gain some traction for simple personal sensors. The market potential is enormous (and scenarios of

several billion installed units are feasible), but the slow adoption rate means it may take decades to ramp up.

The potential for sensor networks is huge and could be relevant for public safety organizations over time, for data overlay and coverage in difficult areas. Whether a sensor network could one day be used as a CCWNI infrastructure is completely unclear at this point. The timeline for the evolution of sensor networks makes it irrelevant to consider for public safety at present.

Available market for infrastructure: Yes, but immature

Available market for terminals: No

Infrastructures in operation within public safety: No.

4.3.5. 802.20 Flarion

The IEEE 802.20 task group has been working on a specifically mobile wireless broadband standard. This group originally included proprietary wireless broadband vendors such as ArrayComm, Flarion Technologies and IPWireless (now NextWave), which already have commercial deployments. However, because of a lack of any real progress, during 2004, this group suffered defections to 802.16e-2005, and the 802.20 standards effort is not expected to survive. 802.20 aims to provide high-speed wireless connectivity to mobile users, even when they are travelling at speeds of up to 250 km per hour.

Available market for infrastructure: No

Available market for terminals: No

Infrastructures in operation within public safety: No.

4.4. Extensions of existing mobile infrastructures

4.4.1. Mobile extensions to GSM/WCDMA

Rivada networks is marketing a solution in the US based on a commercial 3G network provider combined with a mobile local infrastructure that can extend the public network with capacity and coverage in emergency situations. Ericsson markets QuicLink as a technology to be used in setups such as Rivada's.

Requirement name	Mobile extensions Evaluation
Same radio system across all of public safety	N/A
Encryption capabilities	Needs proprietary development
VPN capability	Needs proprietary development
Nationwide coverage	No
Good Voice quality	Unproven
Support Group calls	Needs proprietary development
Support individual calls	Yes
Support data transmissions	Yes, with 3G speeds

Requirement name	Mobile extensions Evaluation
Paging	Needs proprietary development, pagers not available
Traffic prioritizations and alarm calls	No
DMO support	No, but the mobile infrastructure reduces need for DMO.
Integration with other public safety networks	Needs proprietary development
High Availability	Yes, but dependent on the public network service provider in daily situations.
Integration with PSTN's	Yes
Short call setup times	Unproven
End-to-end encryption	Needs proprietary development

Available market for infrastructure: Yes, limited

Available market for terminals: Yes, but not public safety

Infrastructures in operation within public safety: No.

4.5. Existing technologies for public safety mobile infrastructures

4.5.1. Apco Project 25

APCO P25 is a standard for CCWNI, which is reasonably popular in North America but normally not seen outside the Americas. The implementations of APCO P25 are typically regional due to the government structure in the USA. APCO P25 has no nationwide references

The public safety networks in the USA are typically in the 800 MHZ range, where as national public safety networks in Europe utilize parts of the 380 – 400 MHZ spectrum. P25 is, however used by the military in the 380 – 400 MHZ spectrum and therefore terminals are available.

Requirement name	Apco Project 25 Evaluation
Same radio system across all of public safety	Yes
Encryption capabilities	Yes
VPN capability	Yes
Nationwide coverage	Yes, but not proven
Good Voice quality	Yes
Support Group calls	Yes

Requirement name	Apco Project 25 Evaluation
Support individual calls	Yes
Support data transmissions	Yes. Very limited speeds though
Paging	Yes
Traffic prioritizations and alarm calls	Yes
DMO support	Yes
Integration with other public safety networks	Yes
High Availability	Yes, depending on design/implementation
Integration with PSTN's	Yes
Short call setup times	Yes
End-to-end encryption	

Available market for infrastructure: Yes

Available market for terminals: Yes

Infrastructures in operation within public safety: Yes.

4.5.2. TetraPol

TetraPol is a technology similar to TETRA. It is formally a standard but is only supported by one infrastructure technology provider: EADS. It was initially backed by EADS but is not actively marketed any longer. EADS acquired the TETRA operations from Nokia a number of years ago and EADS is now actively backing TETRA while continuing to support existing TetraPol installations.

TetraPol has a significant installed base of app. 90 networks of varying sizes but the last network contract known to Gartner was awarded in 2005 to Federal police in three Brazilian states.

Requirement name	TetraPol Evaluation
Same radio system across all of public safety	Yes
Encryption capabilities	Yes
VPN capability	Yes
Nationwide coverage	Yes
Good Voice quality	Yes

Requirement name	TetraPol Evaluation
Support Group calls	Yes
Support individual calls	Yes
Support data transmissions	Yes, very limited speeds
Paging	
Traffic prioritizations and alarm calls	Yes
DMO support	Yes
Integration with other public safety networks	Yes
High Availability	Yes
Integration with PSTN's	Yes
Short call setup times	Yes
End-to-end encryption	Yes, requires special terminals

Available market for infrastructure: No

Available market for terminals: Yes

Infrastructures in operation within public safety: Yes.

4.5.3. TETRA

TETRA is an ETSI standard, first version published 1995. TETRA is endorsed by the European Radio Communications Committee (ERC) and mandated for use in Europe.

The technical advantages of TETRA when compared to technologies such as GSM include:

- the much lower frequency used gives longer range, which in turn permits very high levels of *geographic* coverage with a smaller number of transmitters, thus cutting infrastructure costs.
- High spectral efficiency - 4 channels in 25 kHz and no guard bands, compared to GSM with 8 channels in 200 kHz and guard bands.
- very fast call set-up - a one to many group call is generally set-up within 0.5 seconds (typical less than 250 msec for a single node call) compared with the many seconds (typically 7 to 10s) that are required for a GSM network.
- Works at high speeds >400 km/h. TETRA was used during the French TGV train speed record on 3 April 2007 at 574.8 km/h.
- the system contains several mechanisms, designed into the protocols and radio parameters, to ensure communication success even during overload situations (e.g. during major public events or disaster situations), thus calls will always get through unlike in cellular systems. The system also supports a range of emergency calling modes.

- unlike most cellular technologies, TETRA networks typically provide a number of fall-back modes such as the ability for a base station to process local calls. So called Mission Critical networks can be built with TETRA where all aspects are fail-safe/multiple-redundant.
- in the absence of a network mobiles/portables can use 'direct mode' whereby they share channels directly (DMO mode).
- gateway mode - where a single mobile with connection to the network can act as a relay for other nearby mobiles that are out of range of the infrastructure.
- unlike the cellular technologies, which connect one subscriber to one other subscriber (one-to-one) then TETRA is built to do one-to-one, one-to-many and many-to-many. These operational modes are directly relevant to the public safety and professional users.

- Equipment is available from many suppliers around the world, thus providing the benefits of competition.
- Network solutions are available in both the older circuit-switched (telephone like) architectures and flat, IP architectures with soft (software) switches.

Its main disadvantages are:

- handsets are more expensive than cellular (about 750 EUR in 2003, about 600 EUR in 2006). This is due to the more difficult technology, smaller economies of scale, and different business model (eg: need for security, high powers and robustness). However cheaper than main (PMR) *competitor technology APCO where prices are >$3000 per handset. TETRA prices expected to fall further as far eastern manufacturers start production in 2007.
- data transfer is efficient and long range (many km), but slow by modern standards at 7.2 kbit/s per timeslot (3.5 kbit/slot net packet data throughput), although up to 4 timeslots can be combined into a single data channel to achieve higher rates whilst still fitting into a single 25 kHz bandwidth channel. Latest version of standard supports 115.2 kbit/s in 25 kHz or up to 691.2 kbit/s in an expanded 150 kHz channel.

Requirement name	TETRA Evaluation
Same radio system across all of public safety	Yes
Encryption capabilities	Yes
VPN capability	Yes
Nationwide coverage	Yes
Good Voice quality	Yes
Support Group calls	Yes
Support individual calls	Yes
Support data transmissions	Yes

Requirement name	TETRA Evaluation
Paging	Possible, but requires special pagers
Traffic prioritizations and alarm calls	Yes
DMO support	Yes
Integration with other public safety networks	Yes
High Availability	Yes
Integration with PSTN's	Yes
Short call setup times	Yes (<500 msec)
End-to-end encryption	Yes, requires special terminals

Available market for infrastructure: Yes

Available market for terminals: Yes

Infrastructures in operation within public safety: Yes.

4.5.4. TETRA2

TEDS is the most well known feature of TETRA release 2 addressing the need for higher data bandwidths putting TETRA roughly on par with GPRS/EDGE. This is under implementation by some providers of TETRA infrastructures.

The bandwith produced by TEDS is, according to Motorola, up to 80 kbps. This is still very limited compared to 3G technologies available in public networks. With Motorola, TEDS requires extra carriers on TETRA1 bases stations and therefore involves a significant investment. According to EADS the base stations does not required a hardware upgrade to support TEDS. Consequently, public safety organizations may choose to stay on TETRA1 and use public wireless broadband infrastructures for high-bandwidth data needs. Up till now, Norway is the only national TETRA network requiring TEDS. The plan is to use it on roughly a third of the base stations.

4.6. Emerging technologies for public safety mobile infrastructures

4.6.1. Project MESA

Project MESA was formed in May 2000 under ETSI. The purpose of project MESA is "producing the specifications for an advanced digital mobile broadband standard much beyond the scope of currently known technologies". Based on a study of the latest draft technical specification[1], the project is eight years after its start still a long way from a technical specification from which providers can start develop technologies. It is therefore way too early to plan for the arrival of CCWNI's based on MESA specs.

[1] ETSI TR 102 653 V3.1.1 (2007-08)

5. TETRA deployments

TETRA Networks have been deployed and are being deployed as nationwide networks in many European countries as shown below in Figure 3. Some of the largest networks in terms of base stations and users include Airwaves network in the UK and C2000 in the Netherlands. TETRA is also used in major cities and regions for public safety purposes. In addition, TETRA is used by many transportation companies as well as airport administrations as a more sophisticated alternative to traditional PMR (Private Mobile Radio solutions). Recently TETRA has become very popular in A/P with a number of planned networks being deployed by e g the Chinese police forces. Also TETRA is being deployed in a number of large airports in India, including Delhi, Bangalore and Hyderabad.

In section 8 is a list of all major TETRA networks known to Gartner.

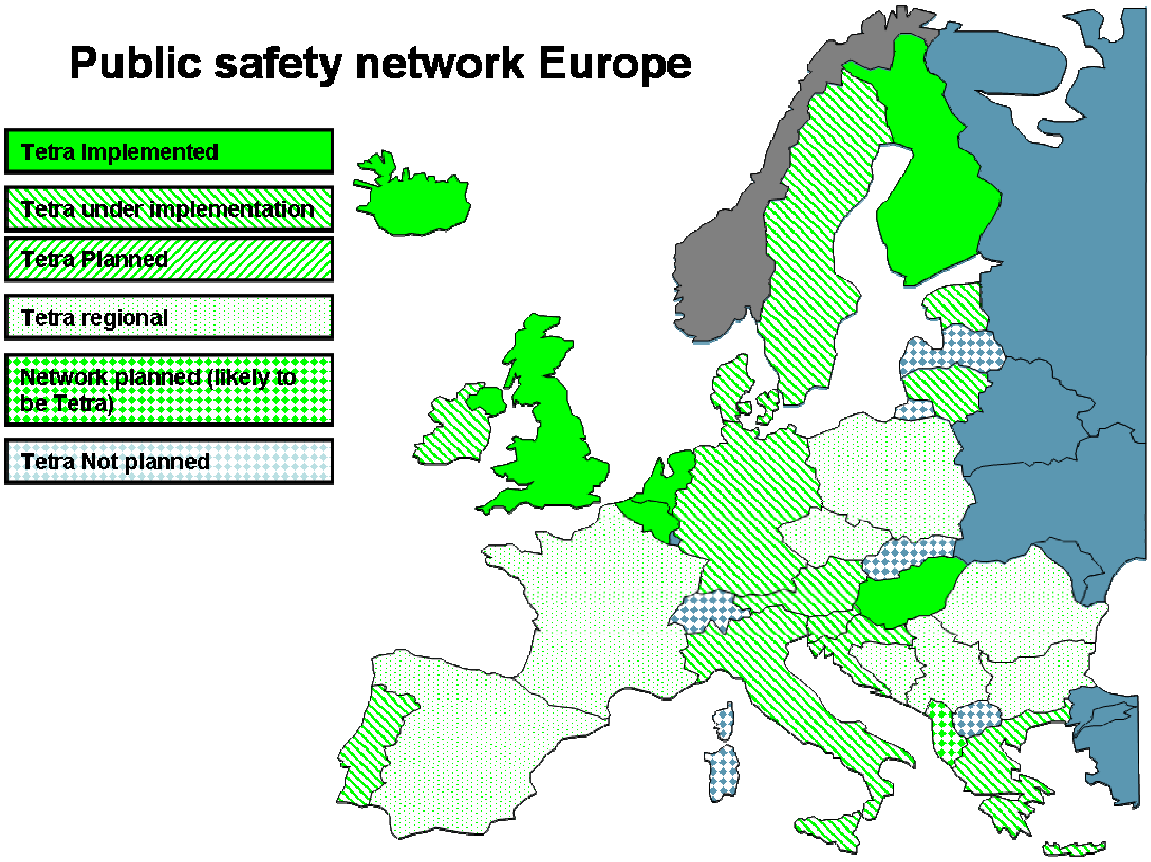

Figure 3: Overview of major TETRA deployments in European countries

TETRAMOU gathers information on awarded contracts and as of August 2007, 1425 contracts were awarded in 103 countries (both terminal and infrastructure contracts).

As a technology for digital CCWNI TETRA is the undisputed leader in Europe and the most widespread digital technology worldwide.

6. Alternatives to TETRA in Norway?

The evaluation of all possibly relevant technologies for providing a CCWNI (Command & Control Wireless Network Infrastructure) has shown the following:

- Only technologies designed to act as a CCWNI meet the essential requirements for such an infrastructure.
- All other technologies existing and emerging would require significant development work on top of the infrastructure to meet the essential requirements.
- None of the technologies would be financially attractive based on a dedicated network for public safety (e.g. building a dedicated GSM or WCDMA infrastructure).
- Using a public GSM/WCDMA infrastructure for public safety is unproven and has large unsolved problems like how to provide traffic prioritization and fast call-setup times. No public safety organization known to Gartner has chosen this solution for a CCWNI.
- Using technologies not designed for CCWNI as a CCWNI would also require development of special terminals that meets the special requirements for public safety people.
- There are no technologies underway to take over the role of TETRA, TetraPol and Apco Project 25 in the near future.

Therefore, three technologies are available that meet the essential requirements for a public safety CCWNI: TETRA, TetraPol, and Apco Project 25. The following can be concluded:

- TETRA is by far the technology with the most traction worldwide for CCWNI. In Europe, all contracts awarded for nationwide CCWNI for the last eight years have been based on TETRA. The last contract for a national CCWNI based on TetraPol was the SIRDEE network in Spain awarded in 2000.
- TetraPol has one infrastructure provider, EADS, which since the acquisition of Nokia's TETRA business markets TETRA as the primary technology for CCWNI. No further development of TetraPol is expected.
- With the current traction on TETRA infrastructures and the length of the awarded contracts, a market for infrastructure technologies and terminals is most likely to be available for the duration of the current contract between the Norwegian Government and Nokia Siemens Networks.
- Apco Project 25 only has traction in USA, and no technology providers actively markets technologies based on Apco Project 25 on the European market[1].
- There are no indications that building a national Apco P25 network would be cheaper than a TETRA network.
- Selecting TetraPol or Apco Project 25 would make integration of infrastructures between Norway and it's neighbouring countries more difficult.

[1] No Apco P25 based solutions has been presented in the latest public procurement processes for national CCWNI's.

In sum, Gartner sees no technologies available on the market that could act as a sensible replacement of TETRA for a CCWNI (Command & Control Wireless Network Infrastructure) for public safety in Norway.

That being said, Gartner expects that public safety in Norway over time will demand commercially available services for higher speed data in the near future.

The technology evaluations undertaken above have not considered the special circumstances in Norway and could therefore be used for any other European country.

One special characteristic of Norway should, however, be mentioned. The Norwegian geography and small population density means that with any technology, providing nationwide coverage is deemed expensive per inhabitant when compared to other countries such as Denmark or Holland.

Attachments

7. Survey questions for decision makers

Questionnaire on essential requirements for public safety communications

1. Which of the following requirements are essential for public safety communications?

Please, for each requirement; answer whether this requirement would be essential, if you were to *invest* in an infrastructure for operational public safety communications *today*?

Requirement name	**Description**	**Is the requirement essential? (Yes, No, Don't know)**	**Comments**
Same radio system across all of public safety	Radio infrastructure will be shared across police, fire, ambulance, and other		
Encryption capabilities	Communication is over-the-air encrypted		
VPN capability	The infrastructure supports more individual organisations communicating securely and inaccessable from other organisations		
Nationwide coverage	The radio infrastructure provides countrywide overage and interoperability		
Good Voice quality	Provides good voice quality in noisy surroundings.		
Support Group calls	Supports geographically and organisationally dispersed group calls.		
Support individual calls	Supports one-to-one calls		
Support data transmissions	Radio infrastructure supports packet-switched data.		

Paging	Radio infrastructure can be used to call out fire personnel.		
Traffic prioritizations and alarm calls	Traffic can be prioritized in overload situations.		
DMO support	The end-user devices supports direct communication without infrastructure.		
Integration with other public safety networks	The radio infrastructure can be integrated with other infrastructures		
High Availability	The infrastructure has high availability in emergency situations		
Integration with PSTN's	The infrastructure can integrate with public telephone networks.		
High-bandwith data	The infrastructure supports high-bandwidth data. (as delivered by 3G)		

2. Which essential requirements are not in the matrix above?

Please list the essential high-level requirements (if any), you would add to the list above:

8. List of major TETRA networks

The following matrix list all major TETRA networks in operation, under implementation or planned known to Gartner.

Country	Location	Nation wide/Local	Implemented / under implementation / planned	Network name
Albanien	Albanien	Nation wide	Planned	
Austria	Østrig	Nation wide	Under implementation	ADONIS
Belgium	Belgien	Nation wide	In operation	ASTRID
Bulgarien	Bulgarien	Nation wide	Planned	
China	Beijing, Kina	Regional	In operation	
China	Wuhan	Local	Planned	
Croatia	Croatia	Nation wide	Under implementation	
Estonia	Estonia	Nation wide	Planned	
Finland	Finland	Nation wide	In operation	VIRVE
France	Lyon, Frankrig			
France	Bordeaux, Frankrig			
Germany	Tyskland	Nation wide	Under implementation	
Germany	Aachen, Tyskland			Aachen pilot
Greece	Greece	Nation wide	Under implementation	
Holland	Holland	Nation wide	In operation	C2000
Hong Kong	Hong Kong Police	Nation wide	In operation	CCIII
Hungary	Ungarn	Nation wide	In operation	EDR
Iceland	Iceland	Nation wide	In operation	
India	state of Andhra Pradesh	Local	Planned	
India	Delhi, Bangalore Ouheydrebad	Local	Planned	
Ireland	Ireland	Nation wide	Under implementation	
Italy	Torino, Italien	Nation wide		
korea	korea	Local	Planned	
Kuwait	Kuwait			
Lithuania	Lithuania	Nation wide	Planned	
Monaco	Monaco	Nation wide	Under implementation	
Norway	Norge	Nation wide	Under implementation	Nödnett
Polen	Warszawa, Polen			C4i

Country	Location	Nation wide/Local	Implemented / under implementation / planned	Network name
Portugal	Portugal	Nation wide	Under implementation	
Qatar	Qatar	Nation wide	Planned	
Romania	Romania	Nation wide	Planned	
slovenia	slovenia	Nation wide	Under implementation	
Spain	Navarra region	Local	In operation	
Spain	Valancia region	Local	Planned	
Sweden	Sverige	Nation wide	Under implementation	RAKEL
Uganda	Uganda	Nation wide	In operation	
UK	England	Nation wide	In operation	Airwave
UK	Jersey, UK	Nation wide	In operation	Airwave
Vatikanstaten	Vatikanstaten	Nation wide	In operation	Vatican City TETRA System
Venezuela	Monagas, Venezuela	Local	Under implementation	

Any questions regarding this report should be addressed to:

Kristian Billeskov
Gartner Denmark ApS.
E-mail: kristian.billeskov@gartner.com

Direktoratet for Nødkommunikasjon Contact Information

Tor-Helge Lyngstøl
E-mail: tor-helge.lyngstol@dinkom.NO