Alternatives for mission-critical services in public mobile networks in Norway

May 2018

TABLE OF CONTENTS

APPENDIX

1 BACKGROUND

In December 2017, the Norwegian Government decided that the 700 MHz radio frequency band shall be made available for commercial operators. This means that a dedicated broadband network for mission-critical use is no longer an option in Norway. This document describes different alternatives for implementing a possible mission-critical broadband system inside commercial 4G/5G mobile networks, based on input from the Norwegian operators.

The present mobile communications network used by the public safety services and preparedness organisations in Norway, is called Nødnett. The network is based on the TETRA standard and was rolled out in the period 2007-2015. It includes about 2,100 radio sites and serves around 55,000 users. The State owns Nødnett, and the responsibility for the network resides in the Norwegian Directorate for Civil Protection (DSB). The daily operation and maintenance is outsourced until end of 2026.

The capabilities of Nødnett cover the needs for mission-critical voice communication and short data messages, but data capabilities are limited by the narrowband nature of the TETRA technology. Nødnett users therefore utilise commercial mobile networks for applications requiring high-speed data, e.g. from police vehicles and ambulances. Currently, these networks do not match Nødnett in terms of coverage or reliability.

DSB is currently doing a concept study for the realisation of a robust and secured broadband data solution to Norwegian public safety and emergency preparedness organisations. It is the vision that in a longer term, the solution will also carry voice services and substitute the present Nødnett. The term “Next Generation Nødnett” (NGN) is used in this paper to describe such a network solution.

There are several questions to be looked into regarding how to implement NGN, including how to define the optimal split of responsibilities between the State and the commercial operator(s). A situation where commercial network(s) carry mission-critical communication is new for the State, the public safety users and the operators. It is therefore essential to involve the affected parties in the process in defining the solution.

2 EXPECTATIONS TO NGN

The expectations to NGN are high, and exceed what the mobile networks offer today in at least these areas:

- Coverage “everywhere”, including tunnels, air-to-ground (for helicopters) and remote areas with limited commercial potential
- High reliability, e.g. availability also during major incidents, extreme weather conditions and various crisis scenarios
- Strong data security and protection against malicious attacks
- Specialised functionality, e.g. for group communication and for communication outside network coverage or when the network is down

All the above needs call for investments in the mobile networks, in particular hardening measures to increase the resilience against power outages and transmission failures. Increasing resilience in tunnel coverage systems (approx. 350 tunnels) to the same level as the present Nødnett will also represent significant costs in Norway.

3 SOLUTION CONCEPTS PROPOSED BY OPERATORS

DSB recently approached the three mobile operators in Norway (Ice, Telenor and Telia) with a Request for Information (RFI), asking the operators a set of questions regarding how they believe NGN should be realised. The RFI covered technical, operational, regulatory and commercial aspects. All operators provided comprehensive answers. DSB also received feedback from infrastructure equipment vendors (Ericsson, Huawei and Motorola) and consultancy companies.

The operators all agreed that utilising commercial mobile networks for mission-critical communications in the future will be feasible, with a possible exception for air-to-ground communication which may require bespoke solutions. The operators had very different views on how an NGN should be realised and what should be the role of the operators, as summarised in the following solution models:

Model 1 – Secure MVNO
The State acquires its own core network and service platform and enters into agreements with preferably all mobile operators for use of their radio access

networks. The basic concept is often referred to as a mobile virtual network operator (MVNO) arrangement. Normally the MVNO's interface to the operators is based on a traditional roaming connection (S8). The "secure MVNO" model is based on the more complex Multi-Operator Core Network (MOCN) interface, whereby sensitive user information such as location and call activity can be concealed from the mobile operator(s). With this model, the State will be responsible for the end-to-end functionality and performance.

Model 2 – A single turnkey provider
A single operator provides NGN communication services through a turnkey contract, and there is no need for any state-owned network infrastructure. If required by the State, the solution can be complemented by national roaming for NGN users in one or two additional radio access network(s) as backup. The preferred operator will be responsible for the end-to-end functionality and performance.

Model 3 – Several competing turnkey providers
This model is an extension to the turnkey model, where two or all three of the operators in Norway can offer NGN services and compete to attract NGN users as customers. The operators must fulfil certain requirements set by the government, before they can offer NGN services. Full interoperability and interconnect on the application level for NGN services, such as Mission-Critical Push-To-Talk, is a prerequisite. When complemented by mutual roaming between the operators, all NGN users will experience enhanced reliability and the same, combined coverage. Each operator will be responsible for the end-to-end functionality and performance of the services for their own subscribers only, but have to co-operate to ensure that services work across the networks.

The three models differ in terms of merits and complexity. Comprehensive studies and considerations are required before a conclusion can be made as to what solution should be chosen for NGN. Several fundamental questions must be addressed, such as:

- Does the State have to own the core network to achieve sufficient level of security and control?
- Should NGN make use of the radio access network from more than one operator?
- How can governmentally funded network hardening be implemented without disturbing the competition between operators?

4 LEVEL OF GOVERNMENTAL CONTROL

By owning the core network and associated service platforms, as with Model 1 (MVNO), the State can have direct control over this most critical part of NGN. Full control over these network elements requires not only ownership, but also that operation and maintenance is performed by a governmental organisation.

In the traditional case, an MVNO only possesses certain parts of the core network, and not the core network elements that control the radio access network. This means that sensitive user metadata such as call activity and location will be visible to the operator of the radio access network. To avoid this, NGN can be implemented with the complete set of core network elements and with MOCN, rather than S8, interface to the commercial radio access network(s). This option implies a significant increase in complexity, both technically and commercially, and represents the most resource and competence demanding solution for the State.

With the turnkey alternatives, Model 2 and 3, NGN can be realised with a separate core network. Separation can be either physical or implemented in software ("network slicing"). In this way, the NGN core network can be managed independently from the rest of the core network infrastructure of the operator(s). This also means that access to the NGN core can be limited to a subset of the operator's personnel, and the sensitive metadata of NGN users can be subject to restricted handling within the operator's organisation.

5 ONE OR SEVERAL RADIO ACCESS NETWORKS

The mobile operators in Norway are close to finalising their planned rollout of 4G coverage. It is expected that two of the operators (Telenor and Telia) each will achieve area coverage figures approaching that of the current Nødnett (86 %), but there will still be areas where one operator provides better coverage than the other does. The third operator, Ice, will cover only parts of Norway with their own network based on commonly used 4G frequencies, but have in addition an overlay 4G network in the 450 MHz band for data communication. Due to the differences between the networks, a solution using two or three networks will provide somewhat better perceived coverage than if

NGN is based on one network only. The service availability will also improve, since the users then often will have an alternative if there is outage of coverage in the primary network. In addition, it is possible to distribute state-funded hardening between the operators, thus avoiding favouring one of them.

With normal S8 roaming, users will experience a 10-30 seconds break in the connection when changing from one network to another, but this will occur only when losing coverage and should normally not be an issue. By using a full-fledged core network and MOCN interface to commercial radio networks, near seamless change of networks is achievable. This will however require close co-ordination of radio parameter settings between the networks and will be a cumbersome solution for the operators to maintain.

Using more than one radio network has some challenges, compared to a one-operator setup. There is an increased commercial and technical complexity, and there may be risk of disclaim of liability in case of failures. Furthermore, additional security issues are introduced, since more equipment and more people are involved.

Individual base station outage is the most common failure in a mobile network. This will not be noticeable for the users in areas where base stations have overlapping coverage. This is often the case in areas with high traffic loads, where all operators have a quite dense grid of base stations. The capacity reduction from outage of one site in such areas will not affect the NGN users noticeably, as long as appropriate prioritisation mechanisms are applied. Still, the ability to switch to another network is useful when several base stations of one operator in an area are down.

The operators often share base station sites, especially in rural areas. This creates dependencies between the radio networks, and failures like power outage or transmission line breaks can affect several or all operators. The same is often the case for tunnel installations. Such dependencies reduce the potential for achieving increased service availability by use of multiple radio access networks.

6 POSSIBLE MARKET COMPETITION IMPACTS

The mobile networks continuously evolve. Market demands, technology improvements and regulatory requirements are typical triggers for the operators' investment decisions. Both consumers and business users will increasingly need and expect more resilient mobile services. Still, it is not very likely that the operators at their own initiative will invest in measures that will fully meet the level of coverage, functionality and resilience expected for mission-critical use, at least not in the short term. Implementing NGN in commercial networks may therefore require a combination of public funding and regulatory provisions. To find the optimal solution requires the assessment of a number of commercial and legal issues, e.g. what agreements to enter into, what regulatory instruments to use, and if changes in legislation will be needed.

All operators should preferably benefit from governmental investments, to avoid introducing competition inefficiencies in the mobile market. To a certain extent, undesirable effects can be minimised by aiming for reinforcing infrastructure elements that represent common vulnerabilities to all the operators. One example is to increase the robustness of radio sites outside the cities, where the operators often share shelters, masts, power grid connections as well as physical transmission lines. Adding redundant transmission and enhancing shared power backup systems at such sites can benefit all operators and consequently all mobile customers as well. Should NGN require new radio sites, governmental funding can be limited to the shareable parts like groundwork, mast, shelter, power, etc., and all operators can be offered to install their equipment irrespective of their NGN participation. Such an approach is applicable to all the three models described in this paper. Still, and regardless of whether NGN will use one or all radio access networks, it may be difficult to make governmental investments that are "non-discriminating" and have exactly the same value for all operators.

7 FURTHER PROCESS

The dialogue with the Norwegian mobile operators has illustrated that there are many considerations to make in order to find the best solution for a mission-critical broadband system inside commercial mobile networks. A number of commercial and technical arrangements are possible, and further assessments are required.

The current Nødnett contracts are valid until the end of 2026. A possible replacement for Nødnett should therefore be in place in due time in order to avoid a situation where negotiating renewal of the Nødnett contract becomes the only option. Full migration to a new system cannot take place until the new system can match Nødnett in terms of coverage, functionality, reliability and security.

It is time consuming to produce the necessary assessments needed for proper governmental decision-making. Comprehensive material for a public procurement process must be prepared, a competition must be arranged and contract(s) must be negotiated. Additionally, operator(s) will need time to implement NGN in their network(s). Nødnett users will have to prepare to migrate to NGN and secure that their control rooms and all other systems can connect to NGN well before Nødnett is switched off.

Before a possible NGN implementation can start, careful assessment of different implementation alternatives, including associated cost and risk, must be performed. Both short- and long-term objectives have to be considered. In parallel, it will be necessary to maintain Nødnett performance until migration to a new solution is completed.

Public safety communication in commercial networks is a cultural change. New value chains must be defined and established. Compared to the present situation with the state-owned Nødnett, the commercial operators have to take on increased responsibility for important functions in society, also during crisis. The State has to find ways to follow up the quality of the services in a network that is no longer under direct State control. The public safety communication system will be more dependent on underlying, commercial infrastructures than it is presently. State investments will come to the benefit of all users of mobile communication.

Both the State and the operators have a lot to learn. All parties must work together to find a win-win solution that will contribute to a safe society in the years to come.

APPENDIX

SUMMARY OF THE OPERATORS' SUGGESTED MODELS

The table below provides a summary of the operators' respective proposals for how to implement a possible "next generation nødnett", NGN. These proposals represent three examples of possible implementation models. Other models can be applicable to NGN.

	Model 1 **State-owned MVNO**	**Model 2** **A single turnkey provider**	**Model 3** **Several, competing turnkey providers**
Main concept	A dedicated, state-owned NGN core network using radio resources in preferably all three commercial networks.	NGN implemented inside a single commercial network. Roaming to back-up radio access network(s) as an option.	NGN implemented independently inside several commercial networks. Full NGN service interoperability and national roaming across the networks.
Main benefit	Governmental control of the core network and user data. Minimum impact on the mobile market competition.	One main responsible, simplest technical and contractual structure.	Enables competition for NGN services. Less impacts on the mobile market competition.
Main challenge	Technically and contractually complex. Many involved parties, need for several contracts. The State must take the end-to-end responsibility.	Hardening the network of the selected operator may result in lock-in and market-inefficiencies.	Continuous risk of service incompatibility and malfunctioning between the networks. Many involved parties, need for several contracts.
Responsibilities and contractual relations	The State is responsible for establishing, updating and operating the core network. Requires separate agreements with the operators for connection to, and use of their radio access networks.	One main contract between the State and a single overall responsible operator.	Separate contracts between the State and the qualified operators. End-to-end responsibility governed by the operators through interconnect-agreements. Public Safety organisations can choose what NGN operator to use.

Norwegian Directorate for Civil Protection

Rambergveien 9
N-3115 Tønsberg
NORWAY

Telephone +47 33 41 25 00

postmottak@dsb.no
www.dsb.no


/DSBNorge


@dsb _ no


dsb _ norge

dsbnorge