Direktoratet for nødkommunikasjon

Type approval of radio terminals

Technical minimum requirements for terminals and key tools

Version 2, 04.04.2016

Contents

1. Introduction

This document describe the Directorate of Emergency communication's (DNK) technical minimum requirements for all TETRA radio terminals in use in the Norwegian Public Safety Network. (Nødnett) These requirements are common for all types of radio terminals, and concern both features that are needed to be able to use the network, as well as important safety features. All type approved terminals must fulfil these requirements, and they are tested when the terminal is type approved. Some of these features are often part of the standard set of features in terminals, and others have to be activated by the use of licenses. I the case of breach of these minimum requirements, DNK have the right to prohibit the use of such terminals, and/ or to disable the terminal.
DNK's technical minimum requirements are meant as a baseline in radio terminal procurements for use in Nødnett, and it is important that all deliveries fulfil these requirements.

DNK have several requirements for the procedures and equipment involved in handling and programming of K and SCK keys. These are requirements to both vendor and distributor of radio terminals, as well as software and hardware involved.

2. Other terminal requirements

The Directorate of Emergency communication's technical minimum requirements covers the basic features of a radio terminal in order for the terminal to be acceptable for use in the network. Other and more functional requirements for radio terminals such as physical size, user functionality, battery lifetime, voice quality and others must be communicated and from the terminal purchaser to the supplier, and is not covered in this document, nor DNK's responsibility.

3. Type approval of radio terminals

All radio terminals used in Nødnett shall be type approved. The type approval includes the terminal hardware and software version, as well as the system/network version. Details about the type approval process as well as an overview of the approved terminal models is available on these web pages:
http://www.dinkom.no/Tjenester/Typegodkjenning-av-radioterminaler/
The type approval is usually done by a standardized test, and the test protocol is available on request from DNK. Here is an overview of the main topics in the testing of terminals:

- Basic registration and deregistration, authentication, change of SCK
- Change of class of encryption, local site trunking
- Transmit inhibit, radio check, ambient listening, stun

- Group call, individual call, telephony call
- Emergency call, tactical and non-tactical
- Mobility: handover, subscriber class, network/country code, power control
- Short Data, (SDS) GPS position report
- DGNA: Dynamic groups, patching
- Callout, end-to-end-encryption
- Gateway/DMO repeater

3.1. Technical minimum requirements

All radio terminals in the Norwegian Public Safety Network (Nødnett) shall have the following features and capabilities:

- Support TETRA standard TR 100 392-17-3, and a frequency range of 380-430MHz
- TEA2 encryption, Security Class 2 and 3, and Subscriber Class according to latest version of Ref. [1]
- Mutual Authentication of radio terminal in network according to latest version of Ref. [2]
- Temporary and Permanent Disable Terminal Kill) according to latest version of Ref. [1]
- Link Budget: Power class 3: ant. gain 2dBi, PC 4: ant. gain 0dBi. Rec. dyn.sens.=-103dBm
- OTAR, Over The Air Re-keying) according to latest version of Ref. [3]
- Static encryption keys (a minimum of 32 SCK) for direct mode (DMO) and for use in base stations in fallback mode, Security Class 2.

The OTAR and SCK requirements can be waived if the terminal in question is not to be operating in base station fallback mode or direct mode. (DMO)

4. Encryption key handling

Vendors and distributors that are capable of delivering equipment with TEA2 encryption algorithms have to establish procedures for secure handling and delivery of encryption keys according to Ref. [3], chapter 6.2.
All procedures and equipment/software must be approved by DNK before use.
As of now, two types of procedures are used for handling K-keys. In cases where the same terminal make is delivered by several distributors, shall all distributors adhere to the same procedures and use the same type of tools.
When testing radio terminals, K can either be generated in Nødnett and transferred to the Reference test system, or have the keys generated in the Reference system, and then have new keys generated in the live system.

4.1. Preferred procedure for handling K key, DNK controls the key equipment

If this is the chosen method, the vendor and distributor must describe the procedure for the following:

- K (and SCK) keys shall be protected in key storage and in the transfer to the radio terminal
- At least two access levels shall be implemented in the equipment:

- Access level for accessing the K keys and K-ref (and SCK)
- Access level for access to keying of radio terminals, but without access to K keys (and SCK)

4.2. Alternative procedure, vendor generates K key

If this is the chosen method, the vendor and distributor must describe the procedure for the following:

- How keys are sent from vendor to DNK (not via distributor)
- System for protection of keys in transport from vendor to DNK
- Deletion of keys at vendor
- Handling of situations of lost keys
- Access control of key handling equipment and software
- Requirements of personnel with access to keys
- Safety measures to ensure that keys are delivered to DNK only
- Key file format, must be possible to import in AuC. (Ref 1)
- Contact point at vendor for DNK personnel in case of questions or problems

4.3. Handling of SCK keys

DNK shall have control of equipment and software for key programming. This equipment can be the same as for handling K keys. Normally, the Nødnett users programming the SCK keys. DNK have the same requirements for this as described in chapter 4.1 above.

5. References

1. TTR 001-01 Version 5.1.1 January 2010, TETRA Memorandum of Understanding (TETRA MoU); TETRA Interoperability Profile (TIP) Part 1: Core
2. ETSI TS 100 392-7 V2.4.1 (2006-10) Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security
3. TETRA MoU Security and Fraud Prevention Group Recommendation 01, edition 4, Authentication Key Distribution

6. Contact details

Please contact DNK regarding terminal type approval and/or technical requirements by email, phone or mail.

Mail address: Direktoratet for nødkommunikasjon, Postboks 7, Nydalen PIB, 0410 Oslo

Email: typegodkjenning@dinkom.no

DNK contact person: Tore Bergvill, phone +47 982 15 245