



# Typegodkjenning av radioterminaler

## Tekniske minimumskrav for terminaler og nøkkelhåndtering

Versjon 2, 04.04.2016



## Innholdsfortegnelse

1. Innledning.....	3
2. Brukerens funksjonelle krav til radioterminaler.....	3
3. Typegodkjenning av radioterminaler .....	3
3.1. Tekniske minimumskrav for radioterminaler .....	4
4. Krypteringsnøkler .....	4
4.1. Preferert rutine for K-nøkkel, DNK kontrollerer utstyr for nøkling.....	4
4.2. Alternativ prosedyre, produsent genererer K-nøkler.....	5
4.3. Håndtering av SCK .....	5
5. Referanser .....	5
6. Kontaktinformasjon .....	5

## 1. Innledning

Dette dokumentet beskriver Direktoratet for nødkommunikasjons tekniske minimumskrav til TETRA radioterminaler som skal kunne benyttes i Nødnett. Kravene er felles for alle typer radioterminaler, og omhandler både egenskaper som gir tilgang til Nødnett og funksjoner som er nødvendig for sikker drift.

Alle typegodkjente terminaler må oppfylle de tekniske minimumskravene, og det blir testet som en del av typegodkjenningen. Noen av egenskapene som omhandles i dette dokumentet er en del av standardutvalget i terminalene, og noen må aktiveres med lisenser. Ved brudd på disse kravene kan DNK forby bruk og/eller deaktivere terminalen.

Direktoratet for nødkommunikasjon har krav til hvordan K og SCK-nøkler til TETRA radioterminaler håndteres. Dette er krav som omfatter radioterminaler, programmeringsverktøy og rutiner hos leverandør og produsent.

DNKs tekniske minimumskrav er ment brukt som basis i anskaffelser av radioterminaler som skal benyttes i Nødnett, og det må sikres at alle leveranser oppfyller disse kravene.

## 2. Brukerens funksjonelle krav til radioterminaler

DNKs minimumskrav til radioterminaler dekker kun basisfunksjonalitet for at radioterminaler kan aksepteres for bruk i Nødnett. Andre og mer omfattende funksjonelle krav som konstruksjon, funksjoner, batterilevetid, lyd kvalitet m.m. må formidles fra bruker/innkjøper til leverandør. Slike krav er ikke DNKs ansvar, og behandles ikke i dette dokument.

## 3. Typegodkjenning av radioterminaler

Alle radioterminaler som benyttes i Nødnett skal være godkjente for bruk i nettet. Godkjenningen gjelder radioterminalens maskin- og programvareversjon samt versjon av Nødnett infrastruktur. Her finner du detaljer om typegodkjenning og oversikt over alle godkjente terminaler: <http://www.dinkom.no/Tjenester/Typegodkjenning-av-radioterminaler/>

Typegodkjenning gjøres som oftest ved hjelp av en standardisert test, protokollen er tilgjengelig på forespørsel til DNK. Her er en grov oversikt over de egenskapene som kan testes i terminalen:

- Registrering, deregistrering og autentisering
- Bytte av SCK og krypteringsklasse, basestasjon i lokalmodus
- Sendersperre, radiosjekk, fjernavlytning, midlertidig deaktivering
- Gruppeanrop, individanrop, telefonsamtale
- Nødsamtale, taktisk og ikke-taktisk
- Mobilitet: bytte av basestasjon, abonnentklasse, nettverk/landskode, regulering av utgangseffekt
- Tekstmeldinger, GPS posisjonsrapport

- DGNA: Dynamiske grupper, sammenkobling av talegrupper
- Utalarmering, ende-til-ende-kryptering
- Gateway/DMO repeater

### **3.1. Tekniske minimumskrav for radioterminaler**

Alle radioterminaler som skal benyttes i Nødnett skal ha følgende egenskaper:

- Tilfredsstillende TETRA standard TR 100 392-17-3, frekvensområde 380-430MHz
- Kryptering (TEA2), Security Class 2 og 3 samt Subscriber Class i henhold til siste versjon av Ref. [1]
- Gjensidig autentisering (Mutual Authentication) av radioterminal til nettverket i henhold til siste versjon av Ref. [2]
- Midlertidig og varig deaktivering av terminalen (Temporary/Permanent Disable/Terminal Kill) i henhold til siste versjon av Ref. [1]
- Link Budget: Power class 3: ant. gain 2dBi, PC 4: ant. gain 0dBi. Rec. dyn.sens.=-103dBm
- Fjernstyrt bytte av krypteringsnøkler CCK (OTAR, Over The Air Re-keying) i henhold til siste versjon av Ref. [3]
- Statistiske krypteringsnøkler (minimum 32 stk. SCK) for direktemodus (DMO) og basestasjoner i lokalmodus (Fallback Mode, Security Class 2)

Krav om OTAR og SCK kan frafalles hvis terminalen ikke skal fungere i basestasjon lokalmodus (Fallback Mode) eller direktemodus. (DMO)

## **4. Krypteringsnøkler**

Produsenter og leverandører som er i stand til å levere utstyr med TEA2 krypteringsalgoritmer må etablere rutiner for sikker håndtering og transport av nøkler i henhold til Ref. [3], kapittel 6.2.

Alle rutiner og utstyr for håndtering av nøkler må godkjennes av DNK før de kan benyttes.

Det er i dag etablert to aksepterte løsninger for håndtering av K-nøkler, og i de tilfeller der samme fabrikat av terminaler leveres av flere aktører i markedet skal samme rutine benyttes for nøkkelhåndtering.

Ved testing av radioterminaler kan K-nøkkel enten opprettes i Nødnett og overføres til testsystemet eller man får egne K-nøkler i testsystemet, for så å få nye nøkler hvis den skal benyttes i Nødnett.

### **4.1. Preferert rutine for K-nøkkel, DNK kontrollerer utstyr for nøkling**

Produsent og leverandør må beskrive følgende:

- K-nøkklene (SCK) skal være beskyttet ved nøkkelsetting og ved lagring i utstyret
- Det skal være minst to tilgangsnivåer til utstyret:
  - Nivå for tilgang til K-nøkler/K-REF (SCK)
  - Nivå for tilgang for nøkkelsetting av radioterminaler, men uten tilgang til K-nøkler (SCK)

## **4.2.     *Alternativ prosedyre, produsent genererer K-nøkler***

Produsent og leverandør må beskrive følgende:

- Hvordan sendes nøkler direkte fra produsent til DNK (skal ikke sendes via forhandler eller leverandør)
- Beskyttelse av nøkler under transport fra produsent til DNK
- Sletting av nøkler hos produsent
- Hvordan håndteres av situasjoner der en radioterminal har mistet nøkkelen
- Tilgangsbegrensning til utstyr som håndterer nøkler
- Krav til personell med tilgang til nøkler
- Hvordan forhindres at nøklene blir utlevert til andre enn DNK
- Nøkler skal leveres i et filformat som kan importeres direkte til AuC. (Ref 1)
- Kontaktpunkt for DNK hos produsent ved spørsmål eller problemer

## **4.3.     *Håndtering av SCK***

DNK skal ha kontroll på utstyret som programmerer nøklene i terminalene. Det kan gjerne være samme utstyr for nøkkelsetting av SCK-nøkler som K-nøkler. Normalt programmerer etatenes driftsorganisasjoner nøkler ved idriftsettelse av radioterminaler. DNK har de samme krav til håndtering av SCK som nevnt for K i kapittel 4.1 over.

## **5. Referanser**

1. TTR 001-01 Ver 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. Kontaktinformasjon**

Kontakt gjerne DNK angående typegodkjenning og tekniske krav. Forespørselen kan sendes via post eller epost:

**Post:** Direktoratet for nødkommunikasjon, Postboks 7, Nydalen PIB, 0410 Oslo

**E-post:** [typegodkjenning@dinkom.no](mailto:typegodkjenning@dinkom.no)

**DNK kontaktperson:** Tore Bergvill, telefon +47 982 15 245