Specification

Nødnett Interface for line connected control rooms

Revision 1.0

January 2026

dsb Direktoratet for samfunnssikkerhet og beredskap

1 Table of contents

1 Table of contents 1
2 Definitions 2
3 Purpose 2
4 Overview of Nødnett, control rooms solutions and roles 3
5 Implementing a control room 4
6 Control room functionality and APIs 4
6.1 IP Addressing 4
6.2 Nødnett Redundancy 4
6.3 Connection to Nødnett Data Centres 4
6.4 Traffic profile 5
6.5 Overview 5
6.6 Voice Communication Service 6
6.7 Short Data Service (SDS) 6
6.8 Location and Presence Services 7
6.9 Radio Commands 8
7 Type approval 9
7.1 Roles and tasks 9
7.2 Test Specification 9
8 Motorola's Application Developer Program 10
8.1 Introduction 10
8.2 Becoming an Application Developer 10

2 Definitions

API	Application Programming Interface, a software interface to connect different software solutions together.
CE	Customer Edge.
CLI	Control Room Line Interface
CRHN	Dimetra Control Room Head Number
DCS	Dispatch Communication Server
DGNA	Direct Group Number Assignment, i.e., dynamically change the talkgroups used by individual TETRA radios.
E2EE	End to End Encryption
GPS	Global Positioning System.
IMW	Intelligent Middle Ware, a platform delivered by Motorola Solutions for providing location and presence services.
HSRP	Hot Standby Router Protocol
ISSI	Individual short subscriber identity, the unique identity used in TETRA networks to identify subscribers.
LIP	Location Information Protocol (TETRA TS 100 392-18-1), an ETSI standard for encoding location data and control.
MGM	Multi-Group Management
PTT	Push To Talk
REST	REpresentational State Transfer
RTP	Real Time Protocol
RUA	Radio User Assignment
RUI	/Radio User Identity
SDS	Short Data Service, a capability provided by TETRA networks that is similar to the GSM SMS service.
SDTS	Short Data Transport Service, the name of the API that provides access to the SDS capability.
TETRA	TErrestrial Trunked RAdio
UNS	Unified Network Services

3 Purpose

The purpose of this document is to provide Nødnett customers and their suppliers an understanding of how control room solutions can connect to Nødnett. The document is for line connected control rooms to be connected to Nødnett using centralised Voice solution.

The Nødnett interface is under continuous development. Please contact DSB to ensure you have the latest version of this document.

4 Overview of Nødnett, control rooms solutions and roles

Nødnett is the nationwide TETRA network for public safety agencies deployed across Norway. In Norwegian, Nødnett means "emergency network".

The Norwegian Directorate for Civil Protection (DSB) owns the Nødnett system on behalf of Norwegian authorities. DSB is a subordinate of the Ministry of Justice and Public Security.

Motorola Solutions is the prime contractor of Nødnett to DSB and provides the network using its Dimetra IP Scalable solution.

In order to meet Nødnett customer needs, DSB offers the product **Control room connection**. This product allows customers to connect their preferred control room solution to Nødnett through a standard Nødnett interface. A Control room connection to Nødnett is useful for customers that wish to follow up and communicate with their Nødnett radio terminal users, or for customers that wish to communicate and control equipment via Nødnett.

Functionality such as voice, short data service (SDS), packet data, radio commands, positioning and terminal status is available to the customer's control room solution through a collection of application programming interfaces (APIs). An overview of the system is illustrated in .

The customer of Nødnett is responsible to source a control room solution that meets their needs/requirements. In addition, the control room solution must fulfil DSBs type approval requirements. The type approval is described in section 7.

The customer's supplier of the control room solution needs to be a member of Motorola's Application Developer Program to get access to the required APIs to be able to deliver a solution that can connect to Nødnett.

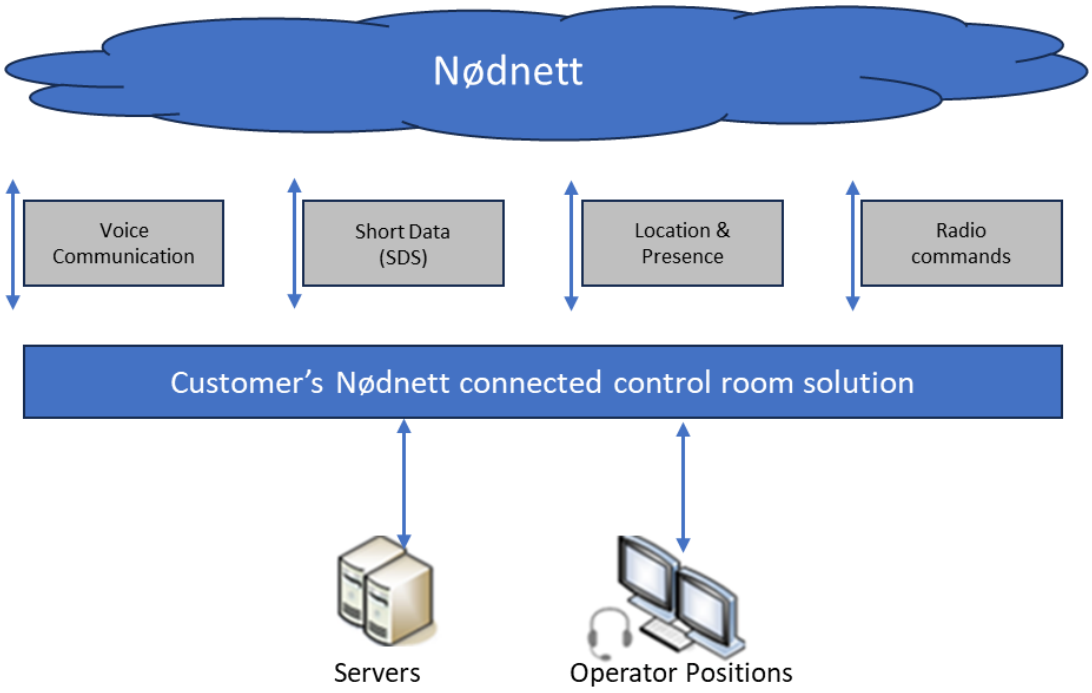

Figure 1 - System overview: Control room connection functionality.

5 Implementing a control room

To connect a control room solution to Nødnett, DSB expects the following process to be followed:

1. Nødnett customers and their suppliers to use this document to understand the control room functionality Nødnett provides and to gain an initial understanding of the APIs used to implement the functionality.
2. Suppliers to propose integration to Nødnett customers based upon this understanding.
3. Following award of contracts between the Nødnett customer and the supplier, the supplier to join the Motorola Application Developer Program. This will give the supplier access to the necessary APIs and corresponding documentation required to implement the customer's requested functionality.
4. Motorola to make available the APIs and the associated technical support to allow the supplier to develop their control room solution, indicating the versions of the APIs that are applicable to Nødnett. The current versions of the APIs are Dimetra 9.1 and IMW 5.2.3. For Dimetra 9.1 only the APIs/functionality in D8.3 is offered, while new functionality in Dimetra 9.1 needs to be clarified/agreed with DSB as these are currently not tested/released in Nødnett.
5. The supplier may choose to use Motorola laboratories to perform initial integration between their control room solution and Dimetra.
6. The Nødnett customer to request type approval from DSB for the specific control room solution to connect to Nødnett.
7. DSB's operations and maintenance organisation to provide configuration guidelines that must be adhered to.
8. The supplier to install and integrate their equipment into the Nødnett customer's control room sites.
9. The Nødnett customer to accept supplier's control room solution prior to go-live.

6 Control room functionality and APIs

6.1 IP Addressing

The IP addressing in Nødnett and connected control room solutions is coordinated through use of private IP addresses and Network Address Translation (NAT). Hence, the control room solutions need to use the allocated private IP addresses, both as source and destination, when accessing services in Nødnett. DSB will provide the private IP addresses to be used.

6.2 Nødnett Redundancy

Nødnett is designed, deployed and operated to provide high resilience and availability for services. Nødnett is a geographical redundant (GR) system with multiple Dimetra zones. All service platforms, including the Intelligent Middleware (IMW), are GR deployed.

The control room solution needs to connect to at least two Nødnett data centres for having redundant connections and to be able to utilize the redundant resources in Nødnett. The two Nødnett data centres represent geographical redundant locations. For large control room solution that requires more than 50 operator positions in Nødnett the control room solution should be able to connect to four Nødnett data centres.

6.3 Connection to Nødnett Data Centres

DSB delivers the connections for customer's locations to Nødnett data centres. The standard solution toady is IPVPN delivered though subcontractors and deliver CE routers (Customer Edge) at the customer location. The IPVPN solution has one primary connection and a secondary connection. A prerequisite for automatically switch between the primary and secondary connection is that the customer provides a LAN connection between the CE routers. In the event of a failure on the primary CE or its connection to

Nødnett an automatic switchover to the standby CE is performed. The switchover may take up to 60 sec.

DSB is working on a new IPVPN solution with the subcontractor to improve the switchover time down to only few seconds.

Nødnett will have the capability of IPSec link encryption of the connections provided by subcontractor of IPVPN. Encryption would be based on pre-shared keys. The customer should have the capability to support IPSec as this may be a requirement in the future.

6.4 Traffic profile

The current delivered IP VPN connections ensures that the different traffic types get the required QoS. The CE router at the customer locations distinguish between different traffic. Hence, the customer does not need to tag the IP-packets.

6.5 Overview

An overview of the functionality, which is available for implementation in control room solutions, is summarized in including the APIs that suppliers can use to access this functionality. Subsequent sections describe the restrictions for the APIs and services in Nødnett. The APIs and the corresponding documentation are available through the Motorola Application Developer Program. Hence, detailed information is not included in this document.

The supplier of the control room solution needs to take into consideration applicable Motorola Technical Notifications (MTNs) for the APIs.
For instance, the MTN-0108A-19-EA is applicable for the MCC7500 SDK and is related to number of simultaneous logins/logouts to DCS console users on the same DCS server.

Functionality	**API**
Voice Communication	Voice Stream MCC7500 SDK A-law encoded PCM over RTP Dispatch Communications Server Audio Packet Definition Document Audio Control Motorola proprietary API using CORBA via TCP/IP, MCC7500 SDK – API Documentation
Short Data (SDS)	Motorola proprietary SDTS-TLX and SDTS-CM-COM protocols on top of TCP/IP Transport Layer - TCP (RFC793) SDTS (Short Data Transport Service) Programmers Guide
Location and Presence	REST API - JavaScript Object Notation (JSON) over HTTP or HTTPS Unified Network Services Locations Interface Control Document Unified Network Services Presence Interface Control Document Unified Network Services MGM Information Data Format Unified Network Services Common Interface Control Document
Radio Commands	Computer-Aided Dispatch Interface (CADI) API Programmers Guide

Table 1- API/Interfaces to Nødnett for Control Rooms.

Nødnett allows many different groups of users to communicate, where those groups can communicate independently of each other or with controlled communication between groups according to requirement. As each Nødnett customer is ‘on-boarded’ onto the network, DSB uses security facilities within Nødnett to ensure the required segregation between customers. In this section, the terms ‘Nødnett user’ and ‘Nødnett radio’ are used to refer to any Nødnett user or radio that a Nødnett customer is permitted to communicate with.

DSB provides the customer with access to the provisioning system. DSB does not offer any API to the provisioning system.

6.6 Voice Communication Service

This interface allows operators of the control room solution to speak with other Nødnett users and to receive status messages.
Nødnett does not offer the following services:

- end-to-end encryption (E2EE) for voice communication services.
- Telephony Interconnect Calls via DCS
- Radio User Assignment/Radio User Identity (RUA/RUI)

A DCS console user provides voice functionality, where each DCS console user is an end point listening to and generating audio. The DCS console user's access rights will be restricted to applicable Talkgroups and ISSIs for the customer.

The customer may decide whether an ISSI shall be associated to the DCS console user (fixed-ISSI) or the login account (user based ISSI). The control room solution connects to a DCS console user using an instance of Motorola's audio control API to control audio. DCS console user receive two or three RTP streams for speaker audio and send one RTP stream for audio from microphones.

Nødnett has no automatic redundancy for DCS console user, but the control room solution may use other DCS console user(s) available instances for redundancy.

Emergency call handling are to be managed by the control room solution through the DCS MCC7500 API. In order to detect the emergency status through the DCS MCC7500 API the control room solution needs to monitor the talkgroups used for emergency calls.

The following need to be managed by the control room solution:

- The CLIs are be distributed over at a number of different location and connected to different zones in Nødnett.
- The Dimetra Control Room Head Number (CRHN) feature may have up to maximum of 50 console users associated. A console user may be associated to maximum 10 CRHNs. A CRHN can only be associated to console users in one zone.

6.7 Short Data Service (SDS)

This interface allows control room solutions to send/receive short data messages to and from other Nødnett users and for callout. Nødnett does support Store & Forward functionality.

The SDTS protocol does not contain a "keep alive" function. A "keep alive" substitution can be used by the control room solution by sending SDS to itself with PID=203 at suitable intervals.

For callout individual addresses radios (ISSIs) is offered. To avoid base station congestion when a high number of the radios are trying send callout acknowledgement the callout needs to be sent in batches. The following approach shall be followed by the control room solution to ensure that all Callout related SDS (Alert, Test, Info, Clear and eventually re-sent messages) sent over the Air Interface are sent out in batches according to the following rules;

1) Individually addressed Callout SDS are sent in batches of maximum C_1 SDS at the same time.
2) There shall be C_2 seconds between batches
3) Steps 1) and 3) shall be repeated until all Callout SDS are sent.

The parameters C_1 and C_2 should be configurable per control room solution issuing the

Callouts. The initial values shall be: C_1=10 and C_2=4000ms. Any other values need to be accepted by DSB.

Nødnett does not offer the following services;

- SDS group message for callout
- end-to-end encryption (E2EE) capabilities SDS.
- Radio User Assignment/Radio User Identity(RUA/RUI)

.

A control room solution may send SDS to Talkgroups (aka. broadcast). All broadcast regions are defined and maintained by DSB. Any use of SDS broadcast shall be discussed with DSB on a use-case basis before implementation/usage to ensure proper defined broadcast regions and efficient use of resources in Nødnett.

For large control rooms with more than 50 DCS console users the following need to be managed by the control room solution;

- Connection to several SDR/S&F servers to obtain the required resilience and availability.
- The ISSIs used for control rooms has a relation to a specific SDR given by the home zone of the ISSI.

6.8 Location and Presence Services

Intelligent Middleware (IMW) delivered by Motorola Solutions provides the APIs for presence and location services.

The control room solution may utilize the Multi-Group Management (MGM) functionality for creating application groups that may consist of a combination of radios, Talkgroups, static groups and other application groups.

Identity Service enables a secure Single Sign-On (SSO) feature for the IMW. Instead of logging to each service separately, a user provides their credentials only once, in return, the Identity Server assigns an OAuth Access Token which is used by the Application Server throughout the authentication session. As long as the user stays logged in, the provided token is the source of authentication. Unlike the other IMW services, the Identity Service has two active instances. Either of these may be used.

Nødnett does not offer;

- Message services
- Context Services
- QoS Services
- Use of Site in requests/subscriptions

The Location functionality[1] records the last reported geographical position for the radios. The IMW supports the use of ETSI LIP and Motorola proprietary LRRP protocols and the API provides the positioning data in a common format independent of which positioning protocol is used by the radio(s). For asynchronous notification, control room solutions can query the last known presence location for a radio instead of subscribing.

The Presence functionality records the last reported presence status for a radio. Similarly, as for locations, the control room solutions can query the last known presence status for a radio instead of subscribing. The presence information of a radio includes attributes like:

- Basic on/off device presence
- Status-Messages
- Talkgroup and radio site affiliation

The control room solution will be provided IMW access rights for all radios (ISSIs) applicable for the customer and one or more static group(s) containing all the radios. To

provide access rights to other customer's radios/Talkgroups there need to be agreements between the customers. The static groups Talkgroups and ISSIs may be in different agency domains in IMW. DSB will provide mapping tables between the IMW domains and the corresponding static groups, Talkgroups and ISSIs. As the agreements may differ for location and presence services, the control room solution should be able to use different IMW accounts for location and presence services. This ensures correct access rights in MW.

6.9 Radio Commands

The CADI API allows control room solutions to send commands to the customer's radios and receiving reposes of the commands from the radios. The CADI API is provided by several MCADI instances in Nødnett. The control room solution access rights will be restricted to applicable Talkgroups and ISSIs for the customer.

Since the radio presence is offered with the IMW Presence API and the emergency status events via the MCC7500 API there are several commands that are not offered. Only the following commands and related responses offered;

- DGNA
- Radio Stun
- Radio un-stun
- Radio Kill

For large control rooms with more than 50 DCS console users the following need to be managed by the control room solution;

- Connection to several MCADI servers to obtain the required resilience and availability.

7 Type approval

All control room solutions must be type approved on the DSB reference system before they are allowed on Nødnett. The purpose of the type approval process is to verify that the control room solution does not harm the network, that it correctly uses standard Motorola interfaces to access the functionality, and adheres to the Motorola API programming Guides (as provided by the Motorola Application Developer Program).

For a supplier seeking type approval against two functionalities, based upon previous experience DSB expects the supplier to spend up to one week installing and performing initial integration on the test system followed by two or three days of type approval testing. However, this duration will vary according to the quantity of functionalities and functions for which type approval is being sought.

Type approval is not a product acceptance test. It is the Nødnett customer's own responsibility to work with their supplier to ensure that the control room solution provides the required functionality and successfully integrates with the Nødnett customer's operating environment and business processes.

7.1 Roles and tasks

DSB is the owner of the type approval process for Nødnett. DSB will provide access to the reference test system and support from system engineers. The supplier shall supply a report summarizing the test results. The Nødnett customer and supplier must provide sufficient technical resources to prepare their solution and perform the test while DSB will observe and approve the test report. DSB will make the final decision on whether a control room solution can be type approved based on results of the test and issue the official approval letter.

DSB will define what documentation must be provided by the control room solution provider prior to the start of certification testing. This will include descriptions of the use of APIs. The supplier needs to produce the test procedure specific to the control room solution under test, and to get the procedure approved by DSB in advance of the test.

DSB has a process on how to handle re-certification of software updates of control room solutions that have previously been certified for the same customer.

7.2 Test Specification

The supplier needs to prepare the test specification for each control room solution, based on an approved standard test specification from DSB. The standard test specification will be sent to the Nødnett customer in due time before testing is planned.
The focus of the type approval process is on login, logout, maintenance of the connection and reconnection mechanisms of the solution – and how the user is informed if there are problems with accessing the network (i.e. how easy it is to identify the root-cause if problems occur). Specific functionality over the network, such as handling of talk groups, different types of calls, status and short data etc. also have to be demonstrated. There is also focus on efficient use of network resources, i.e. voice channels, data capacity on the network, etc. For example, DSB will specify limits on how much data can be sent, or how many channels can be used per call for patch, multi-select etc. Some of these metrics may be included in the standard test specification.

8 Motorola's Application Developer Program

8.1 Introduction

Motorola operates the Application Developer Program to ensure that partners can bring to market innovative applications that add value to network users. This section describes the application developer program and how it relates to implementation of control rooms connecting to Nødnett. Dimetra APIs and corresponding documentation are available to members of the application developer.

Partners join the application developer program for an initial period of 3 years, during which time the partner has access to the specified APIs as well as up to 10 hours of email and telephone support from Motorola. Following that 3-year period, partners can choose to continue membership of the program for further 3 years. Both initial membership and continued membership attract a small licence fee which is used only to administer to the application developer program. Licence fees are payable per API, with fees being available on request from Motorola.

Motorola has gained a vast amount of knowledge of control room implementations for many types of users worldwide, which is available to partners to reduce risk and provide more innovative control room solutions:

- Prior to a supplier joining the application developer program, Motorola can provide guidance on how control room suppliers typically integrate to Dimetra, including use cases of how currently deployed control room solutions meet user requirements using Dimetra APIs, considering aspects such as resilience, security and geographical distribution.
- As part of the application developer program, Motorola can provide tailored guidance on how a particular Nødnett customer's requirements can be met using Dimetra APIs, including recommended best practice techniques.

8.2 Becoming an Application Developer

Join the Application Developer Program here:
http://www.motorolasolutions.com/en_xu/partners/become-partner/application-partner-developer-program.html

depicts the overview of the application process.

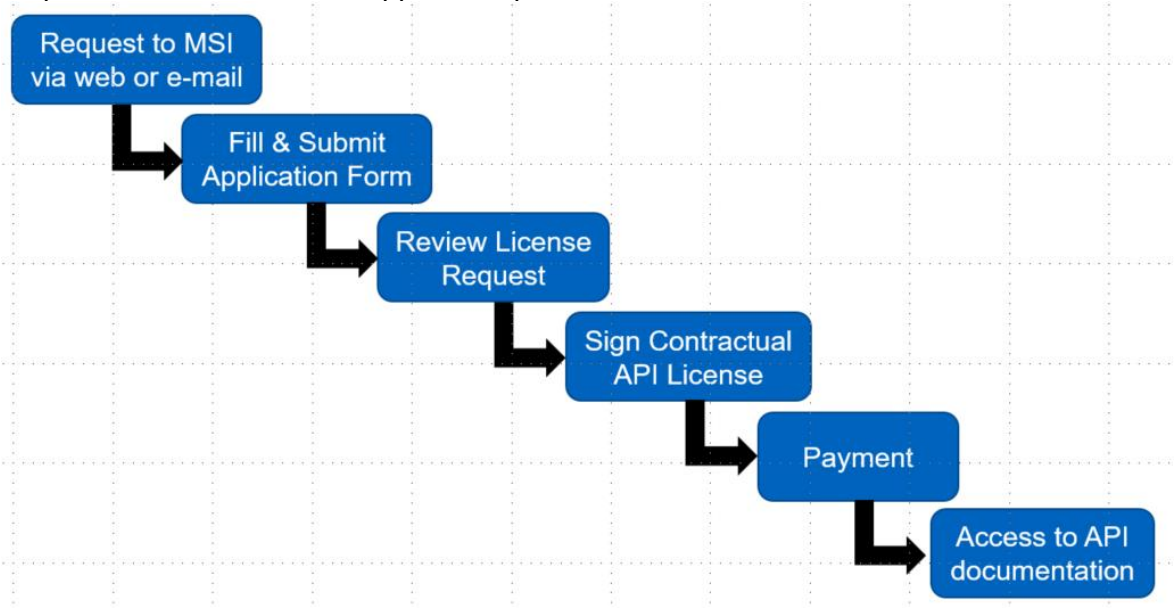

Figure 2 - Overview of the application process.

Include the following information to ensure the correct attention:

- How can we help?: Include the term "Nødnett – New Users"

- Topics of interest: Converged Services, Dimetra

Direktoratet for
samfunnssikkerhet
og beredskap

Avdeling for Nød-
og beredskapskommunikasjon
Postboks 2014
3103 Tønsberg

Besøksadresse:
Nydalen allé 37a
0484 Oslo

Telefon 23 00 57 00

postmottak@dsb.no
www.dsb.no