

RCDS®

REMOTE CRYPTO DISTRIBUTION SYSTEM

The loading and other management of *Cryptographic Variables* (cvs) is a task that has to be performed on a regular basis – often daily – to all radios that need to participate in a secure network.

Today this is performed by manual procedures which often results in military personnel repeating the same procedure at a number of sites containing radio equipment. Often due to the network coverage required by these radio systems the radio sites are unmanned, are in remote locations and often are difficult to access in severe weather conditions. These activities have a high cost for the military in terms of personnel and time.

The *Remote Crypto Distribution System* (RCDS®) offers the ability to perform the management of the cvs to multiple remote sites from a central or mobile manned installation, by making use of the in-country *Digital Data Network* (DDN).

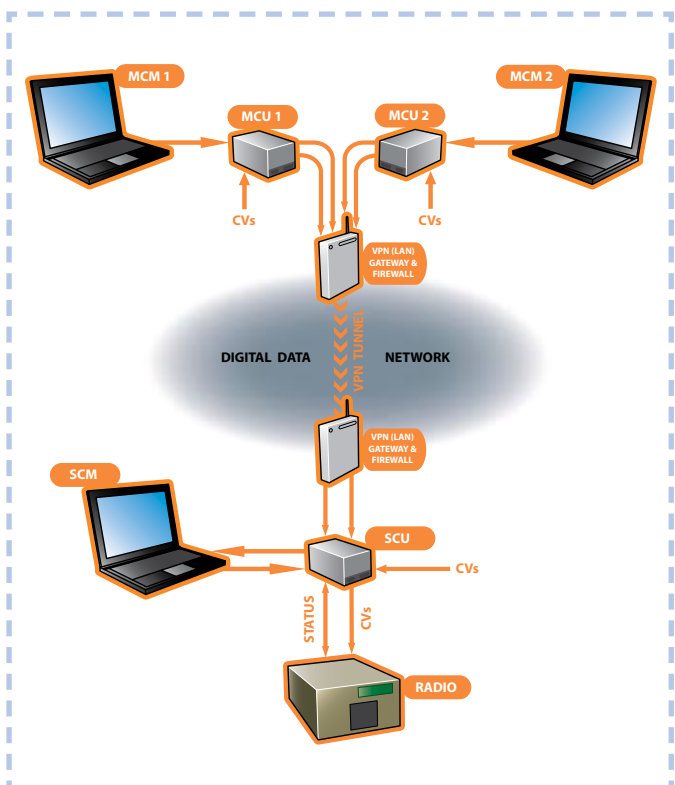
The RCDS® provides the capability to remotely load crypto to multiple remote locations from a central site, obviating the need for manual crypto fill resulting in significant savings on man-power and related costs.

The RCDS® consists of a computer based *Master Crypto Management* (MCM) system which is 'operating-system independent' and normally runs on a laptop. In its basic configuration two small rugged boxes are required, one designated as the *Master Crypto Unit* (MCU) which is normally co-located with the MCM and one designated as the *Slave Crypto Unit* (SCU), which is normally located at the remote site. The MCU and SCU are connected by an IP secure VPN, i.e. in-country *Digital Data Network* (DDN).

The flexibility of the system allows for expansion by simply adding more SCUs for each remote site and if



necessary, multiple MCUs to cater for different operational activities (i.e. c2). At the remote site(s), an optional *Slave Crypto Management* (SCM) system can be installed to enable control of the collocated radio. Note that the system is unobtrusive thus allowing for manual operations or control of crypto fill devices.



Features

- ▶ Open architecture
- ▶ COTS independent
- ▶ Crypto equipment independent
- ▶ Data logging
- ▶ Remote control & monitoring of equipment discretely
- ▶ CV erasure on tamper detection
- ▶ Supports both DS-101 & DS-102 interfaces

Key Benefits

- ▶ Distribution from a centralised location
- ▶ Avoids critical re-keying failures
- ▶ Provides auto crypto accountability
- ▶ Re-keying of remote manned /unmanned sites
- ▶ Increased operational reliability due to the lack of dependency for personnel at remote sites
- ▶ Fast re-keying (error correction)
- ▶ CV loading to radios in different networks
- ▶ Different CV can be loaded to same radio in different positions
- ▶ Remote zeroise
- ▶ Number of radios is unlimited
- ▶ Cost effective

Security

All components of the system have the ability to input, receive from distribution, temporary store and load CVs. A firewall prevents and reports unauthorized access from the computer software. Multiple computers can control the RCDs®, enabling a standby capability. The standby unit receives all ongoing operations information enabling it to assume the role as the active unit on demand.

Master Crypto Management Functionality

The main tasks of the MCM are to control and monitor CVs and the RCDs® equipment. All CV and system activities are automatically logged. This includes short title and expiry dates of CVs, date and time of CV import, distribution and deletion, username of operator, and the system status.

The main task of the optional standby MCM is the capability to assume the role as the active MCM on initiation of the MCM mode switch, either on the active MCM or as a request to the standby MCM.

Slave Crypto Management Functionality

The SCM can be in either active or standby mode. When in active mode it controls the collocated SCU with loading and erasing of CVs. In standby mode, it only displays the status of the co-located SCU.

As is the case with the MCM, all CV activities are automatically logged.

CV Erasure

The MCU and SCU will erase the temporarily stored CVs upon:

- ▶ CVs individually expiring by date and time.
- ▶ A command from the MCM or SCM.
- ▶ MCU or SCU power failure.
- ▶ The MCU or SCU detecting tampering attempt.

Accreditation

The RCDs® was originally approved by the *Norwegian National Security Agency (NONS)* up to and including *HEMME* (Norwegian Secret). Since this approval the RCDs® has successfully completed both *EMC* and *TEMPEST (SDIP-27A)* tests. These tests were the last to be conducted prior to achieving *NATO* accreditation following which it is planned to achieve *USNSA* approval.

Technical Data

Casing for MCU and SCU:

- ▶ H×W×D: 74 × 105 × 142.2 mm
- ▶ Power: 19-36 VDC
- ▶ Tested in accordance with:
 - ▶ *Aerospatiale, HT-GS-B-03-AS/M-2.0* Ariane 5 equipment test requirements
 - ▶ *DnV, 95-1067 EMC* test of SSR
 - ▶ *DnV, DN106-D2654* vibration test
 - ▶ *MIL-STD-461E* EMC
 - ▶ *Tempest SDIP-27A*
 - ▶ *MIL STD 810* vibration / shock

RODIAN Communications AS

International Marketing Agent for Eidsvoll Electronics AS
Fakkeldgården • Postboks 293 • N-2602 Lillehammer • Norway
enquiries@rodiangroup.com
www.rodiangroup.com