DTD II - Data Transfer Device

Part of Cybels KMC Defence

English

THALES
Building a future we can all trust

The Data Transfer Device (DTD II) is a high security embedded device used to distribute, prepare and load crypto material.

DTD II is able to securely store and distribute black and red keys of variable byte lengths.

DTD II - Data Transfer Device

The Data Transfer Device (DTD II) is a high security embedded device used to distribute, prepare and load crypto material, see Figure 1. For an overview of all provided key management services related to the depicted segments, please refer to the Cybels Key Management Centre (Cybels KMC) brochure.

The DTD II is able to securely store and distribute black and red keys of variable byte lengths. The large alphanumeric keypad (43 keys) and display (6 x 20 characters) make the device user-friendly. Its ruggedised housing allows for outdoor use under hostile environmental conditions. The DTD II is secured against the installation of spyware while installing additional applications onto the device to extend its functionality.

Thales' DTD II is used within the Electronic Key Management System (EKMS) of the German Armed Forces as well as NATO and several other European programs.

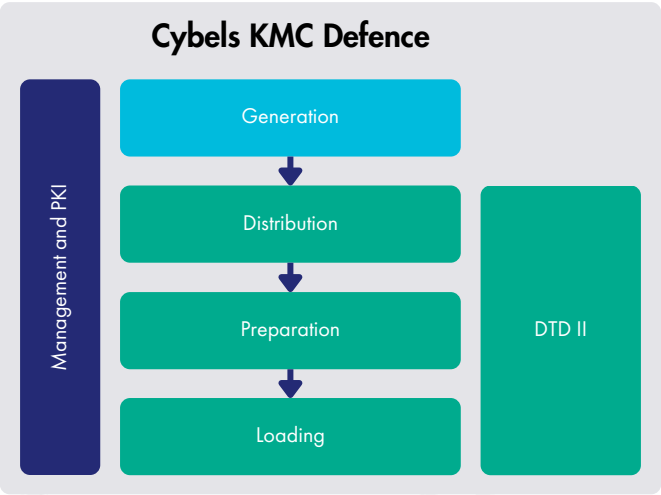
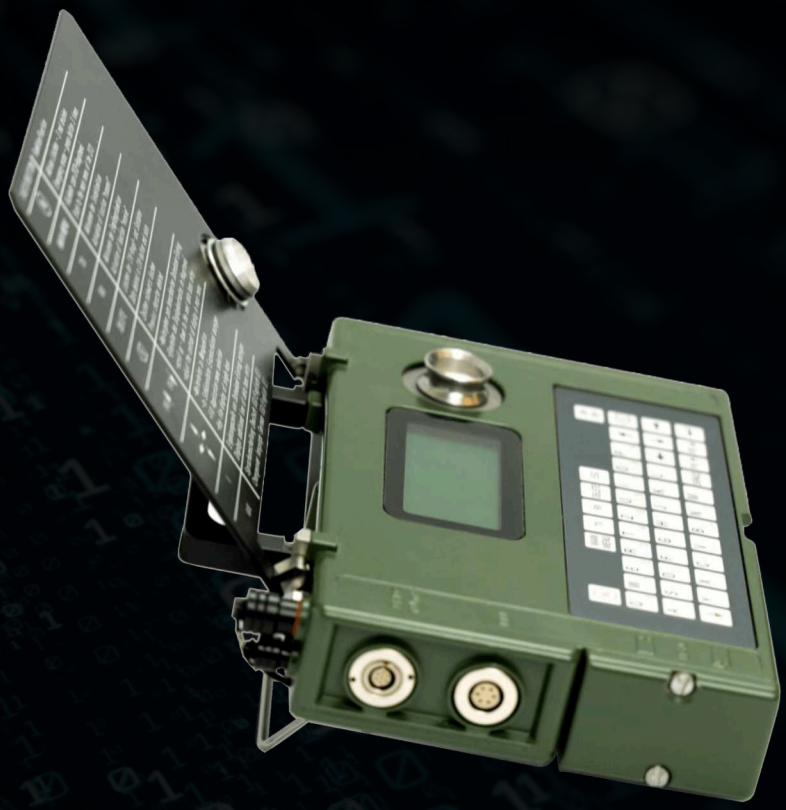


Figure 1 - DTD II in Cybels KMC Defence Portfolio



Main Functions

- Secure storage, transport and transfer of:
  – TRANSEC and COMSEC keys
  – Frequency data and device parameters
- Key and key file management, including tag and key header information in accordance with EKMS 308 Rev F
  – Import, transfer and output via DS-101, DS-102 and RS-232
  – Handling of key files to support distribution tasks
- Records security-relevant events with time and authentication parameters in a user-specific audit log
- Maximum of 8 users with access rights defined by Crypto Ignition Key (CIK)
- Distributes black and red keys of variable lengths
- Replaces KYK-13 and KOI-18 (or KSP1, KLL1) as well as partial functions of the KYK-15
- Additional options to load user specific applications for:
  – Crypto material preparation for specific crypto host, e.g. IFF and MIDS including block upgrade 2
  – Network data management (e.g. frequencies)
  – Device control (e.g. remote keying)
  – Planning and control information, frequency hopping

Interfaces

Ports

- FILL port - for crypto hosts
- Power supply port - 9 Volt DC 150mA
- Crypto Ignition Key (CIK) slot - for removable user access token

Protocols

- DS-101 crypto material transfer, in accordance with EKMS 308 Rev F
- DS-102 Common Fill Device Interface (CFDI), in accordance with EKMS 308 Rev F
- RS-232 crypto host loading, in accordance with EKMS 603

HMI - Human-Machine Interface

- Keypad: 43 keys
- Display: 6 x 20 characters

Physical Characteristics

Temperature

- Operation: -20°C to +70°C
- Storage: -40°C to +70°C

Weight

- 1.75 kg

Dimensions

- Height: 55 mm
- Width: 240 mm
- Depth: 160 mm

Power Supply

- Two 1.5 Volt C batteries
- Optional external power supply

Electromagnetic Compatibility

- In accordance with VG-Guidelines and MIL-STD-461E

Environmental Tests

- In accordance with MIL-STD-810E
  - 500.3 Low pressure
  - 514.4 Vibration
  - 516.4 Shock
- Tested for air transportation up to 10,000 m

Security Characteristics

Classification

- NATO Cosmic Top Secret
- STRENG GEHEIM (German Federal Office for Information Security (BSI))

Accredited to

- TEMPEST: SDIP 27 Level A
- COMSEC: ZDv A-960/1, BSI-Grundschutz, IT-Grundschutzerweiterung Bundeswehr
- BSI-VSA-10420

Export Limitations

- Controlled Cryptographic Item (CCI)

Operational Security

- Removable user access token, Crypto Ignition Key (CIK)
- Tamper protection and detection
- Emergency erasure (zeroization)

Crypto Host Compatibility

- Global Positioning System (GPS) - e.g. Safran GPS GADIRS
- Identification Friend or Foe (IFF) - e.g. Thales TSX 2500 Family
- Multifunctional Information Distribution System (MIDS) - e.g. Datalink MIDS JTRS
- Radio communication - e.g. Thales SEM93
- Crypto computer - e.g. Rohde & Schwarz ELCRODAT 4-2
- Network security - e.g. Thales TCE621

Works with

- ESE - Crypto Material Generation
- VESUV - Crypto Material Distribution and Management
- KPE II - Key Processing Entity
- KLMS - Key Loading Management System
- OCMU - Onboard Crypto Management Unit

THALES

Building a future we can all trust

Thales Deutschland GmbH
Thalesplatz 1 - 71254 Ditzingen - Germany
+49 (0)7156 353-0
E-Mail: de-cybels-kmc@thalesgroup.com
> Thalesgroup.com <