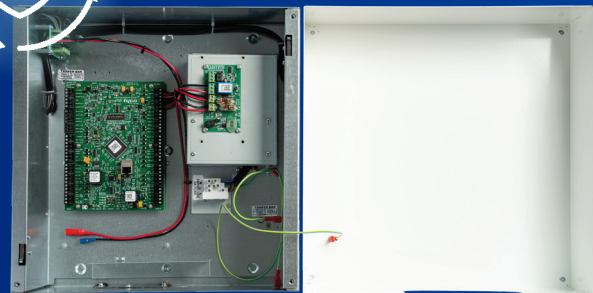


CEM SYSTEMS

DCM 200 - Intelligent Two-Door IP Controller National Protective Security Authority (NPSA) Approved



Intelligent two-door controller

Supports a full two door set (IN/OUT) and up to four NPSA certified OSDPv2 smart card readers.



Secure Communication

Open Supervised Device Protocol Version 2 (OSDPv2) with AES encryption ensures safe, bi-directional data exchange between NPSA approved readers and controller



Reliable Offline Operation

Powerful 32-bit processor and large internal database enables 24/7 access decisions at the door, even without host connectivity.



Secure installation

Supports firewall allow-listing, with rapid IP address configuration via DIP switches, DHCP, or auto-configuration. Encrypted database download of up to 50,000 cardholders in under 2 minutes.



Designed for Security

NIST FIPS 140-3 compliant firmware. High performance deterministic door control process, secure boot, encrypted key storage, IPv4 10/100 Mbps Ethernet host connection & TLS 1.3 between server and controller.



AC2000 NPSA-Rated Component

DCM 200 is a core component of NPSA rated product: AC2000 v13.0 web-based access control system.

Intelligent Two-Door NPSA Controller

The CEM Systems DCM 200 (Door Control Module) is an intelligent two-door controller designed for use within the CEM Systems AC2000 NPSA-approved access control solution. Engineered to interface securely with the AC2000 v.13 web-based NPSA access control platform, the DCM 200 is a key component of a trusted security solution for government facilities and other critical infrastructure environments.

Following successful evaluation under the UK National Protective Security Authority (NPSA) Automated Access Control Systems (AACS) Scheme, AC2000 v13.0 has achieved

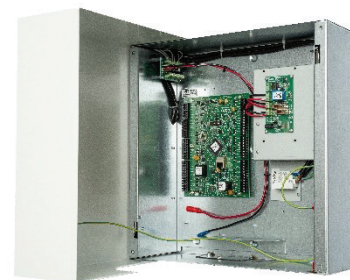
NPSA CLASS assurance and is listed in the Catalogue of Security Equipment (CSE).

The DCM 200 supports up to four NPSA-certified Open Supervised Device Protocol (OSDP v2) smart card readers, enabling secure bi-directional access control for entry and exit across two doors. Powered by high-performance 32-bit processors, the controller performs smart card credential verification and offline access decision-making locally, ensuring uninterrupted operation and continued security even when communication with the AC2000 server is unavailable.

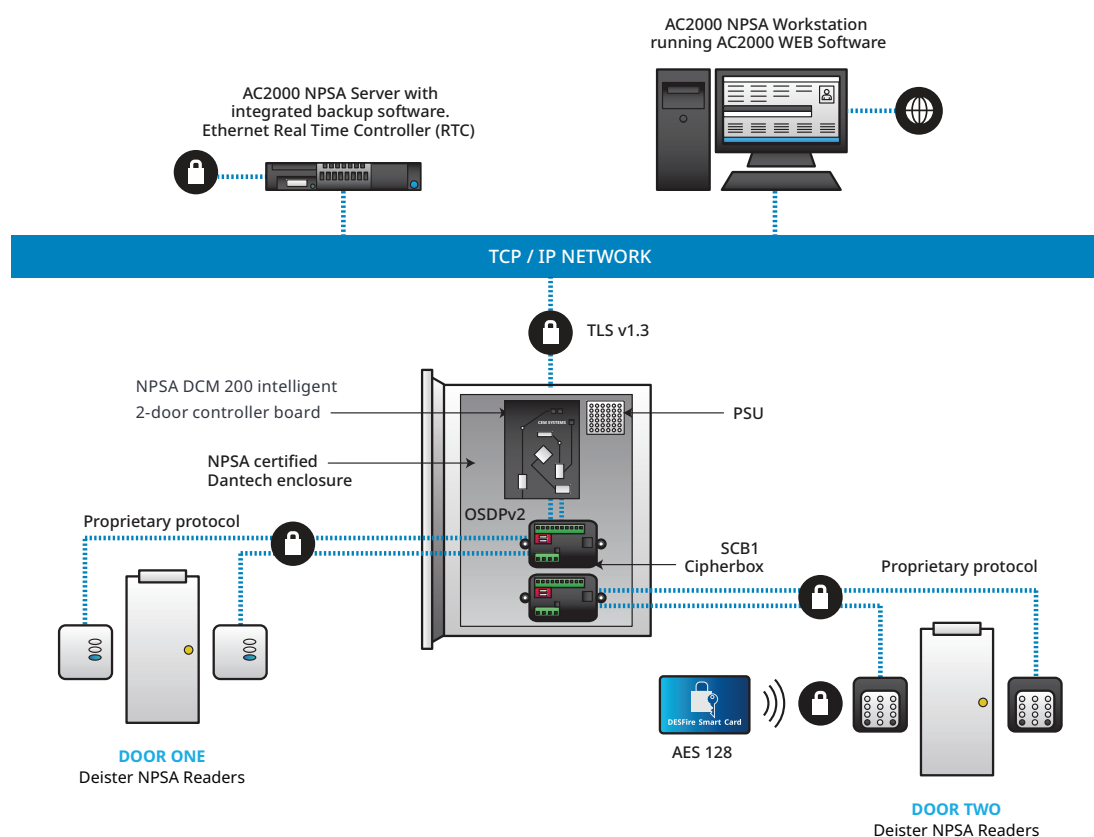
DCM 200 with tamper resistant enclosure

For NPSA-approved installations, the DCM 200 must be deployed within a CEM Systems supplied, NPSA-certified Dantech enclosure, together with a power supply unit (PSU), tamper detection sensor, and an appropriate backup battery.

The DCM 200 (firmware version 9.6.8) is developed in accordance with strict NPSA security and cyber resilience requirements, incorporating multiple layers of protection to safeguard system communications, credentials, and controller operation.



DCM 200 NPSA supports up to 4 OSDPv2 Readers for both IN/OUT control on 2 doors



National Protective
Security Authority

The DCM 200 supports OSDP v2 readers and keypads via RS-485 connectivity. Peripheral devices, including NPSA-approved readers, keypads, credentials, and Request to Exit (REX) devices are not covered by the AC2000 NPSA AACs evaluation and are certified separately through their respective certification schemes.

The AC2000 NPSA-Assured solution has been tested and approved using Deister OSDP v2-compliant devices, including the PRD5/3 Reader or KPD5/3 Keypad Reader with Secure Cipher Box 1/3 (SCB 1/3) and ATS7 or ATS27 tamper plate.

*** AC2000 v13.0 is listed in the NPSA Catalogue of Security Equipment (CSE). Visit the NPSA website for current product assurance and certification details. <https://www.npsa.gov.uk/>**

Security Features at a Glance

- **Hardened Controller Security**

- All unused controller ports are disabled and locked down to prevent attack
- Secure communications between the AC2000 server and DCM 200 are protected using Transport Layer Security (TLS) 1.3 encryption.

- **FIPS 140-3 Compliant Firmware**

- The DCM 200 utilises cryptographic functionality validated to US Federal Information Processing Standard (FIPS) 140-3 requirements.
- All stored controller data and security certificates are encrypted for enhanced protection.

- **Offline Anti-Passback**

- Prevents a credential from being reused on the same NPSA reader until it has been presented at another linked reader or a configurable time period has elapsed.
- Helps deter credential sharing and passback attempts by preventing users from immediately handing an access card to another individual.

- **Offline Wrong PIN Lockout**

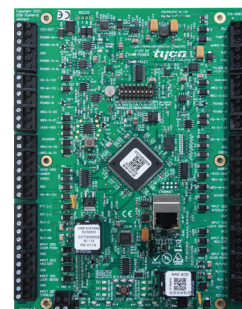
- Supports NPSA compliance requirements by locking a credential after three consecutive incorrect PIN attempts.
- During offline operation, lockout enforcement occurs locally at the controller, with all PIN retry events uploaded to AC2000 once communications are restored.

- **End-of-Life Security**

- Supports secure decommissioning procedures to protect certificates and sensitive stored data throughout the product lifecycle.

- **Network Security Controls**

DCM 200 controllers and AC2000 v13 server and workstations must be assigned to an approved firewall allow-list before becoming visible and operational on the network, ensuring only authorised devices can communicate within the secure environment.



OSDP V2 Support

OSDPv2 is a secure access control systems protocol standard developed by the Security Industry Association for peripheral devices. With added secure AES 128 encryption, it provides bidirectional communications and advanced security features for connecting OSDPv2 compliant card readers to DCM 200 control panels, eliminating the threat of signal interception.

Easy to Install

The DCM 200 is designed to be extremely secure and easy to install. The installer simply adds the controller to the firewall list, configures IP address by selecting DIP switches, using DHCP or auto-configuration, provides it with power, connects to an Ethernet network and the reader self-configures and receives the encrypted database at a rate of up to 50,000 cardholders in under 2 minutes.

Designed for Security

The DCM 200 uses a Secure boot and Secure upgrade mechanism to protect the operation of the system.

The AC2000 NPSA-Assured solution must be installed, configured and commissioned by a CEM Systems AC2000 NPSA Certified Reseller trained and accredited on AC2000 v13.0. All deployment activities must be undertaken in accordance with NPSA security guidance and mitigation requirements.

Installation Web Dashboard

The DCM 200 features a secure onboard Web Dashboard that provides authorised users with access to initial configuration, monitoring, and troubleshooting functions for the controller and connected NPSA-certified devices. Through the dashboard, users can view power, door, input/output, network, and database status, as well as configure network settings and output current limits.

For NPSA deployments, the Web Dashboard is automatically disabled once the DCM 200 is connected to an AC2000 system. Access can only be re-enabled by an authorised AC2000 user with the appropriate permissions and an AC2000 Multi-Factor Authentication (MFA) login using a mobile authenticator application. This additional layer of security enhances identity verification and helps ensure that only authorised and authenticated personnel can configure and manage DCM 200 controllers within an NPSA-assured environment. Furthermore when the NPSA Dantech enclosure is closed, and the dashboard has been re-enabled, the dashboard operates in read only mode.



Specifications

Operational	
Inputs	4 Tamper Supervised Door Inputs (Analogue 2/4 state) per door: • Door Position • Lock Status • Request to Exit (REX) • Interlock (Internal & External Interlock) Unused door inputs can be used for general purpose sensor monitoring. Additional board inputs: • Tamper • Fire • Power Fail Sense Input (for mains fail on the power supply) Automatic door release for Fail-safe locks Spare communication ports are disabled/locked down
Outputs	2 outputs per door: FET and Relay Used to control a NPSA certified locking device Supports fault reporting for Reader power violations *Two Relay output: 9 to 30 VDC @ 2 A with dry contact * Two FET output: Nominal 12 VDC @ 1.5 A Switchable ground Current limited (stabilised) Surge protected
Reader Capacity	Two RS485 OSDP-Compliant readers per door Note: Readers must be NSPA certified and listed in NPSA Catalogue of Security Equipment (CSE).
LED indicators	Power, Link to host, Comms Tx/Rx, Fault / Tamper, Fire, Error, Heartbeat, Reader status LED's, Lock and Relay Status per door
Database Memory	256MB NAND Flash
Database Size	Supports at least 250,000 cardholders and 50,000 offline transactions & alarms
Database records	32bit and 128bit card database records Database AES encrypted Security Wipe: Disabled (System Lockdown) Transaction logs and cardholder records cannot be deleted in accordance with NPSA requirements. Security Wipe function is disabled by default but may be enabled by authorised users for end-of-life security wipe, ensuring no residual security data remains on decommissioned units.

Real time Lock	Accurate RTC with rechargeable battery backup
Card Support	CSN, PSN
Fire Interface Functions	Monitoring of a Fire system dry-contact relay output. Onboard LED indication of status. Firmware event processing and ability to map alarm. Hardware control of all onboard power to release mechanisms (fail-safe)
Configuration	Installation network configuration settings set by Local Secure Web Server. Operational parameters downloaded from host server.
Modes of Operation	• Normal Door Mode • Interlock Mode

Electrical

Voltage – DCM 200 Board & Dantech Enclosure	NPSA certified Dantech enclosure with tamper detection DCM 200 NPSA enclosure is supplied exclusively by CEM with a Power Lite PP-711 PSU (13.7 VDC, 6A, 82W), featuring battery backup/UPS functionality, battery charging, tamper detection, and continuous monitoring of power supply, AC mains, and fault conditions. CEM Supplied Dantech PP-711 PSU only (DC Output 13.7 VDC, 6A)
Current Consumption	DCM 200 Board-only: 231mA @ 13.5 VDC
Power available to door accessories (e.g. Readers, Locks, etc.)	(6A @ 13.7 VDC)
Clock Power Backup	Battery powered, 3.0V rechargeable Lithium Min. 120-hours after power shutdown (IEC60839-11-1)
Backup Battery - Enclosure	Connection for emergency power changeover detection, with a nominal 12VDC operation and provision for charging suitable VRLA battery (not supplied). Evaluated with Yuasa NP7-12 (12V 7Ah) VRLA Battery

Communication

Host System	AC2000 v13.0 WEB software installed on hardened NPSA server
Host Interface	10/100BaseT, Single RJ45 connector
Host Protocol	IPv4 Ethernet, DHCP Support
Reader Interface	2 x Encrypted OSDPv2 RS485 ports with Auto-Detect and Power Sequencing Control for 4 x OSDPv2 NPSA read heads
Security	TLS v1.3 Encrypted Host Communication. Onboard Secure Element for Secure Key Storage. Trusted Boot architecture with locked-down boot sector.

Physical

Dimensions – Dantech Enclosure (with board, battery backup & tamper protection)	404.80 x 402.50 x 123mm (15.94 x 15.85 x 4.84 inches) Or 405 mm x 403 mm x 123 mm (16 in. x 16 in. x 5 inches.)
Weight - Board Only	0.1 kg
Weight - Enclosure	With enclosure & PSU, no battery: 5.0 kg (11 lbs)
Housing	Wall mount 1.2mm Dantech steel enclosure
Housing Colour	Grey

Environmental

Temperature	Operating: -10°C to +55°C (EN50130-5 Class II) Storage: -40° to 60°C AC PSU: -10°C to 55°C (-14°F to 131°F)
Humidity	Operating: 0 to 90% RH non-condensing Storage: 0 to 95% RH non-condensing
Rating	IP Rating: IP3X / IK Rating: IK04

Regulatory

Security	NPSA Class Assured Certification Certified to NIST FIPS 140-3
Agency Certifications	CE
Safety	IEC/EN 62368-1:2014+A11:2017
Emissions	EN-55032:2015 Class A
Immunity	EN-50130-4:2011 + A1:2014
Environment	RoHS, REACH & WEEE

Ordering Information

Model Number	Description
DCM/200/NPSA	DCM200 NPSA Two Door Controller Module – board – with installation in DAN-HS-CEM-12V-4A Dantech enclosure with 12V DC PSU