Product Brief

THALES
Building a future we can all trust

Thales CN700 Series Network Encryptors

Cyber resilience at the tactical edge

thalestct.com

THALES

From the cockpit to the battlefield, the CN7000 series extends certified, military-grade encryption to the most contested environments, safeguarding Command, Control, and Intelligence (C3I) against threats.

In modern defense environments, secure communications are as crucial in the field as they are in core network infrastructure. Thales CN7000 series of quantum-resistant network encryptors extends military-grade network encryption to every location duty calls – from submarine depths to aerial missions – arming military assets with uncompromising protection against sophisticated state and criminal cyber threats.

The CN7000 encryptor series brings exceptional durability and security to the edge, preserving command, control, communications and intelligence even under battlefield conditions.

The CN7000 Series Delivers High-assurance Encryption

Crypto Agility

- Quantum-resistant encryption for future threats
- Toolkit for Custom Ciphers (CSDK) enables deployment of sovereign algorithms to meet future threats and mandates
- Support for evolving encryption standards

Platform Agility

- Protection for all domains
- FIPS-140-3 Level 1 certified OS
- Secures converged IT/OT environments on any platform

Network Agility

- Protects voice, video, and data across any network
- Low-overhead, Layer 2-4 encryption across network topology (unicast, multicast, full mesh)
- Supports unicast, multicast and broadcast traffic
- Flexible topologies: point-to-point, hub-and-spoke, full mesh

Designed for Military Mobility: Land, Sea, Air

Wherever the operation – on land, at sea or in the air – the CN7000 adapts to the mission with a variety of form factors for military uses. Fanless rugged enclosures are designed from the ground up to withstand harsh temperatures, vibration, dust and water, exceeding mil-spec standards (-40°C to +70°C (-40°F to +185°F), IP67). Edge deployments benefit from real-time encryption at speeds up to 10Gbps, ensuring rapid, uninterrupted data flows when and where it matters most.

The Next Generation of Maritime Encryption

Purpose-built to secure naval communications in the most demanding environments – from ship-to-shore operations to real-time data and video transmission.

Designed for deployment across traditional and autonomous vessels, including wind-powered drone vessels, CN7000 will provide advanced encryption for sensitive telemetry and submarine detection data, ensuring mission secrecy across maritime domains. Engineered for resilience, CN7000 extends robust protection from the ocean's depths to command centers on the surface – setting a new benchmark for secure naval connectivity.

The Next Generation of Tactical Land Encryption

Built for modern battlefield mobility, it delivers secure in-vehicle and tactical communications across rugged and dynamic environments.

From voice and video to real-time command and situational data, every transmission is protected within vehicles, convoys, and mobile command hubs – ensuring uninterrupted co-ordination in the field.

Rugged by design, it withstands shock, vibration and unstable power conditions while maintaining near-zero latency for mission-critical operations.

Unbreakable Communications for the Modern Air Domain

Engineered for the demands of modern air force operations, the CN7000 provides secure, real-time communication across all your critical assets. It seamlessly links aircraft, ground stations, command centers, and earth-to-space links, with built-in radiation shielding to withstand the harshest aerospace environments.

Secure voice, video, and mission data are protected, from cockpit systems to UAVs and mobile command hubs. Its resilient design provides uninterrupted operational availability and robust encryption for uncrewed platforms, guaranteeing secure data for critical border patrol, SAR, and disaster missions, regardless of high latency or extreme network conditions.

CN7000 Model Comparison

Defense forces depend on the CN7000 for secure connectivity anywhere, ensuring uninterrupted access to mission-critical data in extreme conditions. Its rigorous engineering delivers peace of mind, allowing commanders to focus on the mission – knowing their communications are protected, resilient and future-proof.

	CN7105	CN7107	CN7108
Maximum speed	Up to 1 Gbps encrypted throughput	Up to 1 Gbps encrypted throughput	Up to 1 Gbps encrypted throughput
Secured Network	M12 X-coded, IEEE 802.3 Gigabit PoE+ (25.5W)	M12 X-coded, IEEE 802.3 Gigabit PoE+ (25.5W)	RJ45, 1 Gbps copper
Cryptographic Security	AES-128/256 encryption, GCM/CTR modes X.509 ECC, ML-DSA, ML-KEM certificates Quantum resistant hybrid encryption Custom Ciphers with Cryptographic SDK (CSDK)	AES-128/256 encryption, GCM/CTR modes X.509 RSA and ECC certificates Quantum resistant hybrid encryption using latest ML-KEM, ML-DSA standards. Automatic key management Custom Ciphers with Cryptographic SDK (CSDK)	AES-128/256 encryption, GCM/CTR modes X.509 RSA and ECC certificates Quantum resistant hybrid encryption using latest ML-KEM, ML-DSA standards. Automatic key management Custom Ciphers with Cryptographic SDK (CSDK)
Ethernet	4 Gigabit Ethernet ports via M12x-coded connectors Local (red), Network (black), Management (LAN) Management (Auxiliary Management)	4 Gigabit Ethernet ports via M12x-coded connectors In compliance with IEEE 802.3at PoE + PSE, maximum 25.5W output on single PoE+ port. Total PoE+ power budget: 100 W. Local (red), Network (black), Management (LAN) Management (Auxiliary Management)	2 x Gigabit Ethernet traffic ports (Local/Network) 2 x Gigabit management ports (LAN/AUX) CPU: Quad-core Intel Processor
Management	Central configuration and management with CM7 Network Manager (CM7). Supports Syslog, NTP, SNMPv1 read only monitoring SNMPv3Q for quantum-safe management. Alarm, event and audit logs. USB port for firmware upgrade. Serial console port with SSH access.	Central configuration and management with CM7 Network Manager (CM7). Supports Syslog, NTP, SNMPv1 read only monitoring SNMPv3Q for quantum-safe management. Alarm, event and audit logs. USB port for firmware upgrade. Serial console port with SSH access.	Central configuration and management with CM7 Network Manager (CM7). Supports Syslog, NTP, SNMPv1 read only monitoring SNMPv3Q for quantum-safe management. Alarm, event and audit logs. USB port for firmware upgrade. Serial console port with SSH access.
Power	Input Power: 160W, 20V/8A Optional: CN7000-PA-160-OW power supply -30°C to 70°C (-22°F to 158°F) DC Input: 8V to 48V DC input (M12 S-coded)	Input Power: 120W, 20V/6A. Optional CN7000-PA-120-OW power supply or for in-vehicle applications, directly from the host environment. Connector: 5.5mm power jack w/locking. Damping bracket. Wall mount (optional).	Input Power: 9V – 42V, up to 3.33A DC input. Connector: 5.5mm power jack w/locking. Power supply unit including universal AC wall mount.
Environmental	Operating: -40°C to 70°C (-40°F to 158°F) Humidity: 10% - 90% non-condensing Shock and Vibration: Complies to MIL-STD-810G	Operating: -40°C to 70°C (-40°F to 158°F) Humidity: 10% - 90% non-condensing Shock and Vibration: Complies to MIL-STD-810G	Operating: -40°C to 85°C (-40°F to 185°F) Humidity: 5% - 95% non-condensing Shock and Vibration: Complies to MIL-STD-810G
Physical	Fanless, passive cooling Weight: 5.8kg (12.78lb) Dimensions: 220mm (W) x 310mm (D) x 90.5mm (H) [8.66" (W) x 12.20" (D) x 3.56" (H)] This unit is tamper-evident	Fanless, passive cooling Weight: 1.9kg (4.18lb) Dimensions: 205mm (W) x 155mm (D) x 58mm (H) [8.07" (W) x 6.10" (D) x 2.28" (H)] This unit is tamper-evident	Fanless, passive cooling Weight: 420g (14.81oz) Dimensions: 132.8mm (W) x 100mm (D) x 34.8mm (H) [5.23" (W) x 3.94" (D) x 1.37" (H)] This unit is tamper-evident
Panels	Front: 2 x M12 X-coded Ports Local (protected-side) & Network (unprotected-side), 2 x M12 X-coded (Device management), 2 x USB 2.0 (A-coded), 2 x COM (A-coded), 8 to 48V DC IN (S-coded), Power button Rear: No connectors	Front: 2 x M12 X-coded Ports Local (protected-side) & Network (unprotected-side), 2 x M12 X-coded (Device management), Power Supply Rear: 3 x USB Ports, 2 x Serial Port, LED Indicators	Front: 2 x USB Type-A, 1.55mm Power jack. 2 x RJ45 (Device Management) Side: 2 x RJ45 Ports Local (protected-side) & Network (unprotected-side) Rear: Power button, 2 x USB Type-A LED
SWAP	Optimized for Size, Weight and Power in-vehicle and mobile deployments	Optimized for Size, Weight and Power in-vehicle and mobile deployments	Optimized for Size, Weight and Power in-vehicle and mobile deployments
Certification	FIPS 140-3 Level 1 (CE Crypto Module)	FIPS 140-3 Level 1 (CE Crypto Module)	FIPS 140-3 Level 1 (CE Crypto Module)
Use case	In-vehicle, field deployments	Industrial, OT networks	Smallest footprint edge sites

Sovereignty, trust and tactical assurance

Governments increasingly recognise the need for true sovereignty and strategic autonomy in data security. The CN7000 enables custom cryptography and sovereign cipher deployment, allowing nations to enforce trust and assurance across all layers of their networks. Using the CSDK, defense can load their own encryption algorithms – never reliant on third-parties or competing national standards.

This sovereignty addresses critical threats – supply chain tampering, export controls, and quantum risk – to safeguard sensitive information and intellectual property from state cyber espionage, and equips defense to anticipate quantum computing risks by deploying quantum-resistant, custom solutions today.

The CN7000 platform agility eliminates standardisation lag, enabling instant response to new threats and rapid compliance with national security and sovereign cryptography mandates.

Mission-critical reliability and seamless integration

Built for uncompromising security and mission-critical reliability, the CN7000 delivers trusted protection for defense, intelligence, and national security agencies. High-performance encryption accelerates data transfers without latency, outperforming legacy software and traditional protocols like IPSec.

Thales network encryption platform supports a broad spectrum of network architectures including MPLS, IP WANs, SDN via Transport Independent Mode (TIM). TIM empowers secure, scalable, quantum-ready encryption without the complexity of legacy tunnel-based models, saving space, bandwidth, and management effort.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com