

KRYPTUS

CommGuard 3

Layer 2, 3 and 4 network encryptor with up to 100 Gbps throughput and post-quantum cryptography.

KRYPTUS CommGuard 3 is a network encryptor operating in full-duplex mode that performs tunnel encryption at layers **2, 3 and 4**, fully protecting all upper layers. It runs over any network that delivers IP connectivity, including satellite links and MPLS backbones. It features a dedicated management interface, independent from the data interfaces, ensuring separation between the two contexts.

CommGuard 3 meets the most stringent security requirements for classified communication between HQ, sites and remote operations. With a tamper-resistant hardware mechanism, it supports standard, proprietary and post-quantum algorithms. For added security, it can be integrated with KRYPTUS KNET HSM for high-security provisioning. Users can establish secure mobile communication using KeyGuardian (portable USB cryptocomputer) or CGApp (mobile VPN application), combined with CommGuard.



100 Gbps

ENCRYPTION WITH
FPGA L100

<10 μ s

INSERTED
LATENCY (FPGA)

L2 · L3 · L4

TRANSPORT
AGNOSTIC

PQC

ML-KEM · ML-DSA
(NIST)

7

MODELS, 1U OR
TABLETOP

TUNNEL PROTOCOLS

IPsec

- Full set of standard algorithms: AES-128/192/256 (CBC, CTR, GCM, CCM), ChaCha20-Poly1305, Camellia, 3DES; integrity SHA-1/256/384/512, AES-XCBC, AES-CMAC.
- Key exchange groups: MODP 1024–8192, ECP 256/384/521, Brainpool 256/384/512, Curve25519, Curve448.
- Hash:** FIPS NIST PUB 180-2 SHA-256, SHA-384 and SHA-512.
- Post-quantum:** ML-KEM-512, ML-KEM-768 and ML-KEM-1024 as key exchange groups (FIPS 203); ML-DSA-44/65/87 certificates and signatures (FIPS 204).
- Customer-defined elliptic curves**, usable for key agreement (ECDH in IKE_SA_INIT), digital signature (ECDSA in IKE_AUTH and certificates) and key distribution. The curve is registered once in central management and becomes available for tunnels, CAs and key distribution.

Noise Protocol

- Key agreement:** EdSafe511, ML-KEM-1024, X25519.
- Payload encryption:** ChaCha20-Poly1305, AES-256-GCM, FlexBlockG12-CSRF (Kryptus proprietary algorithm) and One-Time Pad version (CG3-RT with FPGA and OTP models).
- Hash:** BLAKE2.

SIGINT countermeasure

- Provides protection against traffic analysis attacks by adversaries.

SECURE CRYPTOGRAPHIC PERIMETER

Complete and protected cryptographic perimeter:

- Potted hardware:** the security module and the application processor reside in a single region encapsulated in opaque, rigid resin.
- Secure boot:** verified boot chain.
- Encrypted disk:** all system, configuration, key and log partitions are encrypted (LUKS), with keys held by the security module.
- Active, configurable tamper response:** lid-opening, battery and temperature sensors. The reaction to each event is operator-configurable; the intrusion log and reaction settings reside in a dedicated, non-erasable encrypted partition.
- Zeroization:** upon a tamper event, the security module zeroizes the disk encryption keys, rendering the partitions unrecoverable. Remote and local zeroization of keys and proprietary algorithms is also available.
- Encrypted firmware update:** packages distributed as encrypted bundles (CMS/PKCS#7), with signature verified before installation and a redundant A/B partition scheme.
- Resistant to fault injection and side-channel attacks.

CENTRALIZED MANAGEMENT

Centralized management platform (BBCentral) that integrates, in a single solution:

- Fleet management:** secure provisioning (SZTP/BRSKI), certificate enrollment (EST), key distribution, dynamic configuration and batch firmware updates.
- Asset and address management (IPAM):** inventory, equipment lifecycle and organization of IP addressing across the entire fleet.
- Full monitoring:** metrics and telemetry collection, security event correlation, configurable alerts and dashboards, bringing together in one platform the capabilities that would normally require three separate security monitoring, metrics and visualization tools.

ALGORITHM EMBEDDING KIT (AEK)

Service and integration kit for customer proprietary algorithms:

- Symmetric:** embedded as a kernel module, integrated into the device encryption stack and registrable in the IPsec algorithm list.
- Asymmetric:** custom Weierstrass elliptic curves (256–1024 bits), usable for key agreement, signature and key distribution.
- In FPGA hardware:** documented extension architecture for embedding symmetric algorithms in FPGA models.

BUILT-IN SELF-TESTS (BIST)

The device runs built-in self-tests of the hardware and cryptographic algorithms, on demand and at startup. Self-test failures are logged and signaled by a dedicated SNMP trap, and also reflected on the front-panel LED and display.

Models and cryptographic performance

TECHNICAL SPECIFICATIONS

MODEL	DESCRIPTION	PORTS	INSERTED LATENCY
CG3-RT	Secure VPN network encryptor, tabletop form factor	6× RJ-45 1 Gb, 2× USB 2.0, 1× WAN/OTP (SFP+) 10 Gb	~30 μ s
CG3-RT with FPGA	Advanced processing for heavy algorithms	6× RJ-45 1 Gb, 2× USB 2.0, 1× WAN/OTP (SFP+) 10 Gb	~30 μ s
CG3-RT with FPGA and OTP	One-Time Pad tunnels for top-secret communications	6× RJ-45 1 Gb, 1× USB 2.0, 1× WAN/OTP (SFP+) 10 Gb	~30 μ s
CG3-OC	Entry version, ideal for multiple tunnels	1× RJ-45 1 Gb, 2× USB 2.0, 4× SFP+ 10 Gb, 1× QSFP 40 Gb	~30 μ s
CG3-OC with FPGA L10	With U45N, supports 4× 10 Gbps encryption	1× RJ-45 1 Gb, 2× QSFP 10 Gb	<10 μ s
CG3-OC with FPGA L40	With U45N, supports 2× 40 Gbps encryption	1× RJ-45 1 Gb, 2× QSFP 40 Gb	<10 μ s
CG3-OC with FPGA L100	With U45N, supports 1× 100 Gbps encryption	1× RJ-45 1 Gb, 2× QSFP 100 Gb	<10 μ s

- For CG3-OC series models with FPGA Lx, bandwidth capacity can be expanded by purchasing a license for the higher-performance models, with no hardware replacement.
- A redundant packet processing unit can be added to these models.

- All SFP+/QSFP interfaces refer to the slots available on the device, allowing single-mode or multimode transceivers.
- Ruggedized versions available for CG3-RT and CG3-OC.

PERFORMANCE

Connectivity	IEEE 802.3 network
Topology	- Multipoint to multipoint - Resilient peer-to-peer topology - Unit redundancy - Multiple configurable Ethernet ports - Hub-and-Spoke
Operating modes	- Bridge, gateway, transport and tunnel modes - Simultaneous IPv4 and IPv6 support - Jumbo Frames support
Network attack countermeasures	- DDoS detection and protection mechanism: rate limiting of traffic directed to the device, broadcast traffic limiting and control plane with isolated processing - Resistant to broadcast attacks

KEY MANAGEMENT

Key renewal	- Automatic and continuous - Ephemeral asymmetric keys
Key distribution	PKI and PSK based
Interfaces	- Web-based GUI, accessible via IPv4 or IPv6 - Command-line interface (CLI) via executable or SSH, with interactive or single commands
Entropy source	Hardware random number generator (TRNG) compliant with the AIS 31 P2 profile

DEVICE MANAGEMENT

On device	Front panel with 2x20-character LCD display on CG3-OC and CG3-RT models
Remote or over network	- Web GUI and command interface for remote access and auditing - Central security, provisioning and monitoring management - Automated remote configuration - SNMP and Syslog for SOC/NOC integration
Reports	- Access information - Physical or network attack attempts - Automatic e-mail alerts - Traffic statistics per site and aggregated
Remote actions	- Secure remote and/or local firmware update - Remote and/or local device reboot - Local and/or remote key destruction - Local and/or remote proprietary algorithm destruction - Full unit provisioning

POWER SUPPLY

CG3-RT	12V DC input with AC power supply (optional redundant) included
CG3-OC	- Automatic redundant power supply, 100 to 240 VAC @ 50/60 Hz. AC input. - Optional redundant power supply, 36 to 72 VDC. DC input.

ENVIRONMENT

Standard versions	- Operating temperature: 0 to 45 °C - Relative humidity: 10 to 70% (non-condensing) - Storage temperature: -25 to 70 °C
Ruggedized versions	- Operating temperature: -10 to 60 °C - Relative humidity: 10 to 95% (non-condensing) - Storage temperature: -25 to 70 °C

CONFIGURABLE FEATURES

- Routing protocols on internal and external interfaces - DHCP function - QoS function - VLAN function - Replay protection - NAT support	- Cryptographic algorithm suite - Report and alert generation - Firewall function and encryption filters* - Redundancy function - NETCONF and TACACS+ services
--	--

MANAGEMENT AND INTEGRATION

- NETCONF** for programmatic device configuration.
- TACACS+** for centralized authentication, authorization and accounting (AAA), with group mapping, caching and server availability monitoring.
- SNMP v2c/v3** with broad support for industry MIBs: System Group (RFC 3418), IF-MIB and extended IF-MIB (RFC 2863), IP Forwarding Table (RFC 4292), TCP-MIB (RFC 2012), UDP-MIB (RFC 2013), RMON2-MIB (RFC 2021), IPv6-MIB (RFC 2465), SNMPv2-MIB (RFC 3418) and VACM-MIB (RFC 2575), plus the Kryptus proprietary MIB, with traps for intrusion, self-test failure, key creation/destruction/import, authentication failures, CPU usage, disk space, network state and service failures.
- Syslog** for SOC/NOC integration.

DIMENSIONS

MODEL	WIDTH	HEIGHT	DEPTH
CG3-RT	240 mm	44.5 mm	213 mm
CG3-OC	420 mm	45 mm	325 mm

- CG3-RT: compact enclosure with optional adapters for 19" 1U rack. Dimensions also apply to the FPGA variants.
- CG3-OC: 19" 1U rack enclosure. Dimensions also apply to the FPGA variants (L10, L40 and L100), same enclosure.

PHYSICAL SECURITY

- Tamper resistance and tamper evidence
- Voltage, temperature and lid-opening sensors with configurable zeroization
- Ruggedized option for CG3-RT and CG3-OC models

