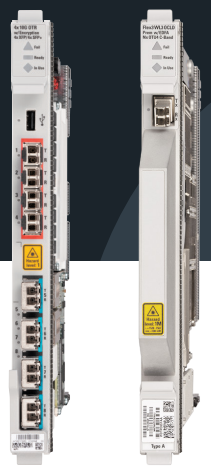
DATA SHEET

High-capacity Wire-speed Encryption Modules

For the 6500 Packet-Optical Platform



Designed to ensure the confidentiality of in-flight data, Ciena's 6500 Packet-Optical Platform cost-effectively enables a flexible 10G, 100G, or 200G protocol-agnostic, wire-speed encryption solution that combines ease of operation and administration to enable a simple-to-implement data protection strategy for Ethernet, Fibre Channel, SONET/SDH, and Optical Transport Network (OTN) services.

Ciena's WaveLogic Encryption solution combines proven encryption technology, deployed on platforms that have a large global installed base, with the proven reliability of the market-leading 6500, deployed by more than 600 operators around the globe. Operators can benefit from a solution that simplifies the deployment of encryption by integrating encryption functionality directly into the network element within the transport network, reducing network complexity and eliminating the need to manage different encryption solutions for various applications.

A Highly Secure and Certified Solution

As part of Ciena's multi-layer security approach that ensures the confidentiality, integrity, and availability of data in the network, encryption is always enabled in Ciena's WaveLogic Encryption solution, ensuring the highest level of security, as all traffic is always encrypted. Although the ability to turn encryption on or off may seem like added flexibility, simple human error can result in sensitive traffic being sent over the network unencrypted. The solution is validated externally and independently certified by a third party to ensure it is implemented with the standards-based AES engine and algorithms. Meeting the highest recognized security standards, which include Common Criteria and FIPS certification, the solution provides a FIPS-certified AES-256 encryption engine with standards-based authentication mechanisms (such as X.509 certificates), enabling operational simplification with seamless integration into existing enterprise PKIs.

Features and Benefits

- Offers an ultra-low-latency wire-speed encryption solution for highly secure and transparent end-to-end communications
- Features protocol-agnostic encryption, offering flexibility to support a variety of services
- Secures all critical in-flight data via FIPS-compliant Advanced Encryption Standards (AES256) encryption solution
- Leverages two distinct sets of keys for authentication and data encryption functions, with a fast encryption key rotation interval of seconds
- Integrates seamlessly into existing enterprise Public Key Infrastructures (PKIs) using X.509 certificate-based authentication
- Enables secure management of Encryption-as-a-Service capability by the end-user in carrier- or enterprise-managed infrastructures via an integrated management tool
- Delivers a field-proven encryption solution widely deployed across the globe in finance, utility, healthcare, military, and government networks

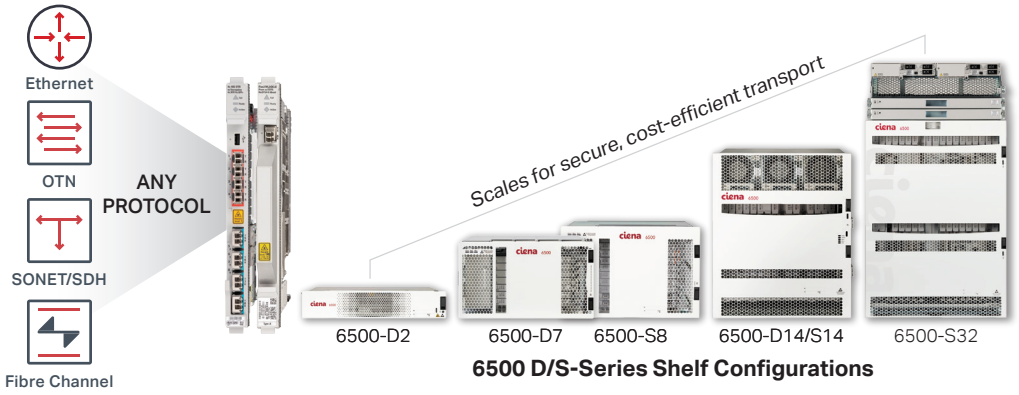


Figure 1: 6500 protocol-agnostic, wire-speed WaveLogic Encryption solution that scales to meet your network requirements

Unmatched Flexibility

With the flexibility of the 6500, customers can select the optimal shelf size to best meet their site-specific capacity, space, and power requirements for cost-efficient transport of encrypted services. An additional key benefit is that the solution is fully protocol-agnostic, supporting a wide range of flexible clients to address multiple applications among security-conscious customers. Customers can deploy differentiated services with ultra-low-latency connectivity and several path/equipment protection options.

Encryption Testing and Certification
Download infobrief

Ironclad Encryption

For enhanced data protection, two distinct and independent sets of keys are used for authentication and data encryption functions, with a fast encryption key rotation interval of seconds instead of minutes. The AES-256 data encryption session keys are autonomously negotiated and rotated every second, independently on each line port, without impacting traffic or throughput and without user intervention. Operators can deploy the next generation of public key cryptography algorithms with support for Elliptic Curve Cryptography (ECC), which provides a significantly more secure strategy than first-generation public key cryptography systems.

Figure 2. 4x10G OTR with Encryption module

10G Wire-speed Encryption

Operators can cost-effectively offer 10G encrypted services by leveraging the single slot 4x10G Optical Transponder (OTR) with encryption module that enables 40G of wire-speed encrypted service capacity via four distinct, protocol-independent encrypted line ports. This FIPS 140-2 Level 3-compliant module provides enhanced protection for critical information against physical tampering via zeroisation; all data is set to zero the moment any physical tampering of the cryptographic module is detected, even when the card is not plugged into the shelf.

Programmable 100G or 200G WaveLogic Encryption

Ciena's WaveLogic Encryption solution leverages industry-leading WaveLogic coherent technology to enable a high-capacity, flexible, and customizable encryption solution via a new WaveLogic 3 (WL3) Extreme line module. WL3 Extreme builds on the capabilities of WL3 and provides extreme performance for all coherent networking applications through the use of additional modulations and enhanced mitigation of

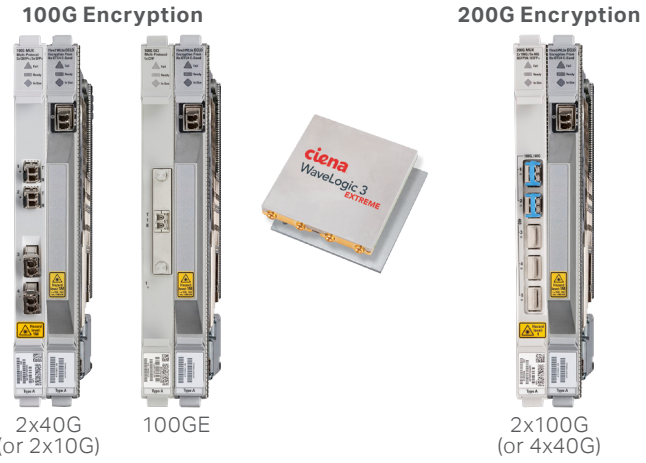


Figure 3. Examples of programmable 100G or 200G wire-speed encryption with WL3 Extreme line module

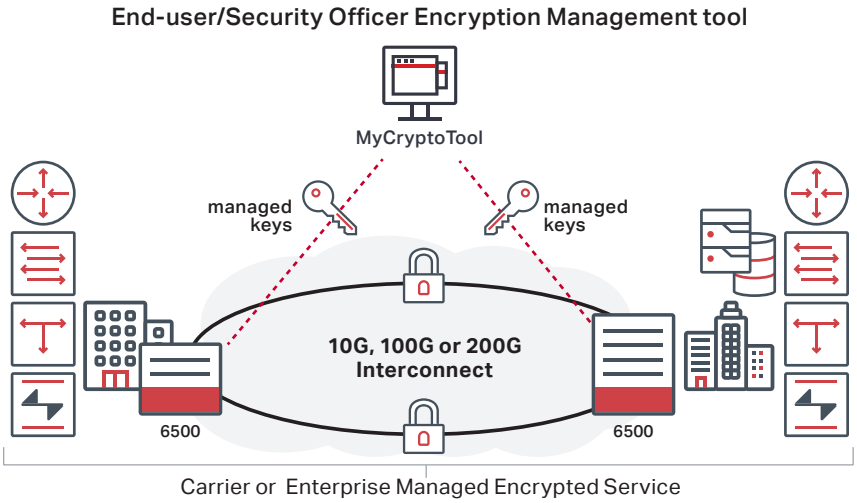


Figure 4. MyCryptoTool dedicated encryption management interface

Data Security with Optical Encryption
Download Infographic now

both linear and non-linear impairments. This cutting-edge solution addresses all infrastructure requirements, from metro to long-haul, and provides software-programmable modulation to enable both 100G encryption with QPSK modulation and 200G encryption with 16QAM modulation—an industry first.

By integrating this WL3 Extreme line module with any one of various client interfaces, operators have the flexibility to deploy a solution tailored to meet their specific traffic needs, be it 10G, 40G, or 100G service transport. As demands increase, the same WL3 Extreme line module can be programmed to carry 200G of encrypted traffic simply by adding an additional client card. Additionally, operators can deploy high-capacity encrypted services across the network by leveraging the 6500's high-capacity hybrid packet/OTN fabric, maximizing the efficiency of network resources.

Encryption Management Made Simple

Ciena's WaveLogic Encryption solution includes MyCryptoTool, a dedicated encryption management interface designed for distributed management of the network that enables the end-user/security officer to independently manage the security parameters and alarms of 10G, 100G or 200G carrier- or enterprise-managed services. MyCryptoTool is a user-friendly interface that securely connects to the cryptographic module and provides mutual authentication, limiting access to authorized security personnel.

Ciena's WaveLogic Encryption solution combines a high degree of flexibility and security with ease of operation and administration to enable a cost-effective, protocol-agnostic, 10G/100G/200G ultra-low-latency encryption solution for securing virtually all of today's web-scale communication applications.

Wire-speed Encryption
Solution application note
Download now

Technical Information

Circuit Pack	4x10G OTR with encryption	WaveLogic 3 Extreme line module with encryption
System Requirements	Operates in any 6500 S/D-Series chassis	Operates in any 6500 S/D-Series chassis except for the 6500-D2
Port Format **Client supported interfaces**	OC-192/STM-64 10GbE LAN, 10GbE WAN FC400, FC800, FC1200 OTU2, OTU2e	OC-192/STM-64 10GbE LAN, 10GbE WAN, 40GbE, 100GbE FC800, FC1200 OTU2, OTU2e, OTU3, OTU4, ODU-Flex
Line supported interfaces	OTU2 OTU2e	Coherent 100G (QPSK); 1xOTU4 Coherent 200G (16QAM); 2xOTU4
Protection Options	1+1 line protection 1+1 client and equipment protection	1+1 line protection 1+1 client and equipment protection
FEC Modes	G.709 compliant RS-8 FEC, UFEC, and OFF	Soft FEC
Environmental Characteristics Operating Temperature Relative Humidity Altitude	 +41° F to +104° F (+5° C to +40° C); +23° F to +131° F (-5° C to +55° C) short term – for 6500-D2/D7/S8/D14/S14 +23° F to +122° F (-5° C to +50° C) short term – for 6500-S32 5% to 85% (non-condensing) 13,000 ft; 4000 m	
Physical Characteristics	11.34 in (H) x 0.99 in (W) x 9.34 in (D) 288 mm (H) x 25 mm (W) x 237 mm (D)	
Security features	• NIST certified AES-256 encryption solution for data encryption • Elliptic Curve Cryptography (ECC) algorithms • Diffie-Hellman secured key negotiation (including Elliptic Curve) • X.509 certificate support for authentication • Support for Certificate Revocation List (CRL) • Hitless AES-256 key rotation every second • TLS-secured and mutually authenticated interface for encryption management • Radius authentication support • TACACS+AAA • SNMPv3 support	
	• 2048-bit RSA certificates • Elliptic Curve certificates	• Elliptic Curve certificates
Certifications	• Common Criteria Network Device Collaborative Protection Profile • BSI (German Federal Office of Information Security) • FIPS 140-2 Level 3 – Certificate #2379, #2635 • FIPS 197 – AES–256 – Certificate #2963, #2964, #3599, #3600 • IBM GDPS • EMC, Brocade	• Common Criteria Network Device Collaborative Protection Profile • BSI (German Federal Office of Information Security) • FIPS 140-2 Level 2 – Certificate #2697, #2843 • FIPS 197 – AES–256 – #3601, #3602, #4231, #4232, #5241 • IBM GDPS • EMC, Brocade

Visit the Ciena Community
Get answers to your questions