Our world is subject to extraordinary levels of threat; there are threats to global and national security; threats to law and order; threats to corporate and individual financial stability and threats to personal safety and privacy. In addition, our world is becoming increasingly reliant on mobile communications technology. High-speed wireless communications help keep us active, agile and informed. The need for secured communications is paramount in today’s ever evolving environment.

STRINGENT SECURITY STANDARDS
Many federal government agencies - such as the Department of Defense and Homeland Security, the Federal Bureau of Investigations, the Secret Service and others - must be in strict compliance with standards. Other federal, state and local government agencies - as well as enterprises such as medical centers and financial institutions - are subject to critical standards for sensitive but unclassified information. These include the Federal Information Security and Management Act (FISMA) and the Federal Information Processing Standard (FIPS) 140-2, as well as industry standards such as the Health Information Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) standards for credit card information protection.

CRYPTR 2 FOR WIRELESS ENCRYPTION
To remain in operation, wireless networks must be in compliance with the relevant standards for their specific mobile communications applications and usage. This can be challenging. Many legacy networks may not have the new encryption technology needed for compliance. Other networks must be upgraded as standards change and become more stringent. CRYPTR 2 Broadband IP Encryption solution is a remarkably cost-effective, easily deployed drop-in hardware solution that provides end-to-end encryption for networks, bringing them into compliance with FIPS 140-2, HIPAA and other mobile security regulations.

STANDARDS-COMPLIANT ASSURANCE FOR PTP, PMP AND MESH NETWORKS
CRYPTR2 encryption is a hardware solution ideal for complementing and strengthening built-in encryption in point-to-point, point-to-multi-point and mesh wireless networks. CRYPTR2 enables the network to meet stringent assurance standards such as FIPS 140-2.
SOLUTION BRIEF
CRYPTR 2 BROADBAND IP ENCRYPTION SOLUTION

SIMPLE, COST-EFFECTIVE PROTECTION FOR CRITICAL MOBILE COMMUNICATIONS NETWORKS

THREATS TO COMMUNICATIONS
Mobile communications networks carry some of the most valuable information in the world:

- Mobile military communications networks on the battlefield transmit crucial tactical information, including orders, troop movement data, and situational strategies that must never become vulnerable to network intrusion.

- Drones flying over enemy territory wirelessly transmit photographs of potential targets, highly classified data that must not fall into other hands.

- An undercover officer in a large city uses a mobile device to send information back to headquarters, a situation in which security can truly be a life-or-death necessity.

- A medical center with a famous politician or celebrity as a patient must protect his or her medical information from hackers who wish to use the data for personal gain.

- A bank or investment firm wirelessly transmitting clients’ personal financial data must guard that data against potential identity theft and stolen credit card and account numbers.

CRYPTR 2 SOLUTION
CRYPTR 2 IP Broadband Encryption solution is a high assurance system that is simple to use and easy to install, and enables mobile networks to comply with a range of federal government standards. CRYPTR 2 provides security compliance with FIPS 140-2 standards for sensitive yet unclassified data. CRYPTR 2 system is a hardware-based solution, offering high bandwidth, allowing for simple installation and management, and delivering end-to-end wireless network security. In addition, it offers highly tamper resistant construction and the same degree of ruggedization criteria as hand-held devices to ensure reliable usage under the most difficult and extreme field conditions. CRYPTR 2 units are also lightweight, present a small footprint and have low power requirements.

DROP-IN UPGRADE
CRYPTR 2 system provides drop-in encryption that enables operators to continue leveraging their investments in current networks. The solution meets information assurance requirements by significantly upgrading built-in security capabilities of typical cellular and other non-FIPS-compliant wireless systems. Units are equipped with both Ethernet and USB interfaces for easy installation and to support connectivity with a broad range of endpoint devices and wireless modems. The result is a simple network-wide data encryption that provides powerful standards-compliant protection with exceptional ease and cost efficiency.

END-TO-END SECURITY
CRYPTR 2 encryption works by creating a secure tunnel through the vast unsecured spaces in a wireless network. Units are installed at either end of the network. Data is loaded and encrypted in a trusted space at one end, then captured and decrypted in IP-enabled trusted space at the other. CRYPTR 2 creates a network layer Virtual Private Network (VPN) that protects data in the IP packets transmitted over the system and is easily configured using a desktop or laptop computer, encrypting data to Level 2 assurance levels for FIPS 140-2 compliance.

THE FIPS 140-2 STANDARDS
The Federal Information Process Standard (FIPS) Publication 140-2 specifies security requirements for cryptographic solutions that are used by mobile network operators to protect sensitive but unclassified government, corporate and personal information. The FIPS 140-2 standard defines four levels of security, ranging from commodity-grade computer solutions at Level 1 to Level 4 which provides standards for protection against physical network intrusion.
CRYPTR 2 is a high bandwidth security solution, providing up to 20 Mbps throughput over standard IP networks. The system’s broadband capabilities are fully compatible with a wide variety of 3G and 4G mobile networks, including point-to-point, point-to-multi-point, mesh WiFi, WiMAX, microwave and modern military tactical network technologies, including multi-hop, multi-modal networks. CRYPTR 2’s bandwidth rates support rich media content including high-speed data, voice and video applications. The solution also incorporates SNMP to support secure network management and diagnostics.

KEY MANAGEMENT
CRYPTR 2 supports Enterprise Key Management System (EKMS), taking keys from Motorola solutions devices. The solution supports remote key management from Motorola’s Key Management Facility (KMF) enabling over-the-network keying and device disabling functions. CRYPTR 2 utilizes Elliptical Curve Key Exchange to ensure suitability for Homeland Security and coalition interoperability.

strongSwan VPN CONCENTRATOR CONNECTIVITY
CRYPTR 2 is interoperable with strongSwan VPN servers. A strongSwan VPN server can be used as a VPN concentrator for CRYPTR 2 allowing for many CRYPTR 2s in the field to communicate securely back to the home network. CRYPTR 2 can accept Elliptic Curve Certificates.

CRYPTR 2 SECURITY SCENARIOS
How can CRYPTR 2 be used to prevent network intrusion and data stealing in real world situations? Among a host of challenging situations, here are a few examples of how network operators can rely on CRYPTR 2 to provide high-assurance and enhanced assurance mobile network encryption protection.

Tactical Command and Control Networks
The Department of Defense is rapidly increasing its reliance on mobile communications. The agency is using mobility for to disseminate and share critical operational and tactical information via voice, data, and video. CRYPTR 2’s low cost, small form-factor, light weight and ruggedized construction makes it an excellent choice for upgrading these tactical networks to meet the standards of FIPS 140-2.

Sensor Systems and Networks
Ground, facility or infrastructure sensor systems are typically unattended and often located in areas that do not allow use of a computer on which a software encryption system can be installed. In many cases, they also involve transmitting data over multi-modal, multi-hop networks that often include mesh WiFi networks using high bandwidth point-to-point or satellite links to transmit data from remote areas to a central processing point. The hardware-based CRYPTR 2 solution is installed at both the sensor end and the control center to provide end-to-end data protection.
SOLUTION BRIEF
CRYPTR 2 BROADBAND IP ENCRYPTION SOLUTION

Perimeter Security
Facilitates such as military bases, college campuses, airports and seaports typically utilize fixed and mobile wireless networks to provide instant notification of perimeter intrusions and other security issues. Because CRYPTR 2 is a hardware-based encryption solution, units can be installed with IP-enabled video cameras, sensors and a wireless modem, providing end-to-end network security.

Commercial Cellular Network Security
Virtually every organization that has mobile workers from federal government agencies to state and local law enforcement departments to enterprise wide field and sales forces relies to some extent on usage of commercial-grade cellular phone networks for mobile communications. CRYPTR 2 solution allows these users to secure communications over public networks by installing CRYPTR 2 with a cellular modem at one end in vehicles or fixed installations and at the other in the mobile command center.

THE CRYPTR 2 ADVANTAGE
For a wide range of mobile network operators with a growing need to secure data, the CRYPTR 2 hardware-based system can be the optimum encryption solution. Costing a fraction of traditional encryption solutions, CRYPTR 2 works with virtually all network technologies, computers and modem types. The solution provides an end-to-end network protection that complies with virtually every important standard. It also offers high bandwidth, ruggedized construction and exceptionally simple installation with a small footprint, light weight and low power usage.

For more information on the CRYPTR2 end-to-end mobile network encryption solution, contact your Motorola Solutions representative or visit our website at motorolasolutions.com/cryptr

Motorola Solutions, Inc. 1301 East Algonquin Road Schaumburg, Illinois 60196, U.S.A. 800-367-2346 www.motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2015 Motorola Solutions, Inc. All rights reserved. (10-2015)