**Microsemi and Athena Announce the TeraFire Hard Cryptographic Microprocessor for PolarFire "S Class" FPGAs, Providing Advanced Security Features**

**Powerful Data Security Technology Enables High Performance and Low Power for Communications, Defense and Industrial Applications**

ALISO VIEJO, Calif., April 6, 2017 /PRNewswire/ -- Microsemi Corporation (Nasdaq: MSCC), a leading provider of semiconductor solutions differentiated by power, security, reliability and performance, and The Athena Group, Inc. (Athena), a leading provider of security, cryptography, anti-tamper and signal processing intellectual property (IP) cores, today announced Athena's TeraFire® cryptographic microprocessor is included in Microsemi's new PolarFire™ field programmable gate array (FPGA) "S class" family members. As the most advanced cryptographic technology offered in any FPGA, the TeraFire hard core provides Microsemi customers access to advanced security capabilities with high performance and low power consumption.

The need for increased cybersecurity has been recognized industrywide, particularly throughout the communications, defense and industrial markets. Athena's highly secure TeraFire cryptographic microprocessor technology addresses these requirements, offering a comprehensive selection of the most commonly used cryptographic algorithms, including all those allowed for military/government use by the U.S. National Institute of Standards and Technology's (NIST's) Suite B, up to the top secret level, as well as those recommended in the U.S. Commercial National Security Algorithm (CNSA) Suite.

The TeraFire cryptographic microprocessor also supports additional algorithms and key sizes commonly used in commercial Internet communications protocols such as TLS, IPSec, MACSec and KeySec. The core has been leveraged in both application-specific integrated circuit (ASIC) and FPGA implementations since its introduction eight years ago, and the inclusion of differential power analysis (DPA) countermeasures in the PolarFire FPGA core is designed to increase its popularity with both defense and commercial customers.

"Microsemi has long provided the best security for FPGAs, and the addition of Athena's TeraFire core takes this to a whole new level in solidifying our strong leadership position in the market," said Bruce Weyer, vice president and business unit manager at Microsemi. "PolarFire 'S class' devices are the only FPGA family that allows users to leverage the Athena TeraFire hard crypto microprocessor. It supports a large number of popular algorithms where every algorithm that uses a secret key is available with strong DPA countermeasures. Microsemi's decision to offer this as a hard core makes designing complex security protocols extremely easy."

Microsemi's highly secure, cost-optimized PolarFire FPGAs offer the industry's lowest power at mid-range densities with 12.7 Gbps Serializer/Deserializer (SerDes) transceivers, as well as high reliability, enabling applications including smart connected factory, functional safety, secure communications and weaponry. The TeraFire cryptographic microprocessor enables significantly better built-in cryptographic capabilities in comparison to any SRAM-based FPGAs and is popular with both defense and commercial customers for its flexibility and efficiency.

The TeraFire core delivers state-of-the-art countermeasures against side-channel analysis (SCA) techniques such as DPA and differential electro-magnetic analysis (DEMA) that could otherwise be used to extract secret keys from the device. Every supported algorithm using a secret or private key is available with countermeasures against SCA. With the Department of Defense's emerging mandate for strong DPA countermeasures, Microsemi's PolarFire devices are expected to see strong adoption by defense customers as a result.

"We are pleased to once again collaborate with Microsemi, which has recognized the need to provide FPGA users with the most advanced security features," said Pat Rugg, Vice President of Sales and Marketing at Athena. "The inclusion of the Athena TeraFire core in its PolarFire FPGAs demonstrates Microsemi's commitment to markets that require high performance cryptographic algorithms, and continues the strong relationship our two companies have leveraged for several years."

According to the new market research report titled, "Hardware Encryption Market – Global Forecast to 2022" from Markets and Markets, the hardware encryption market is expected to be valued at nearly $414 billion by 2022, at a CAGR of 29.3 percent between 2016 and 2022. The major factors driving the growth of this market include increasing concern for data security issues and privacy of data, growing requirement of regulatory compliances, expansion of digital content and significant advantage over software encryption technology.

More than a dozen security-focused certifications have been granted to the TeraFire cores present in each Microsemi PolarFire "S class" FPGA family member under the NIST Cryptographic Algorithm Verification Program (CAVP). Covering the most commonly used algorithms and key sizes, PolarFire FPGAs have the largest number of certifications for built-in cryptographic implementations of any programmable logic device according to the
Additional key features of Athena's TeraFire core and Microsemi's PolarFire "S class" FPGAs include:

- The Athena TeraFire EXP-5200B DPA-resistant cryptographic microprocessor capable of nearly 200MHz operation, implementing all Suite B, CNSA and additional widely used algorithms
- Enabling high-speed DPA-resistant cryptographic protocols at speeds well over 100 megabits per second, using the TeraFire crypto microprocessor for data security and anti-tamper applications
- Integrated true random number generator for generating keys on-chip and for protecting cryptographic protocols against replay and other attacks using fresh random nonces and initialization vectors
- NIST CAVP-certified implementations of the most widely used cryptographic algorithms, modes and key sizes including AES-GCM, SHA-2 and four types of digital signatures
- The TeraFire crypto microprocessor is extensible with additional object code licensed from Athena or with accelerators attached to it via the PolarFire FPGA fabric, for Suite A algorithm support or even higher performance, for example
- "S class" PolarFire FPGAs include a Rambus/Cryptography Research Incorporated (CRI) DPA patent library pass-through license enabling additional DPA-resistant algorithm implementations designed by customers, or from Athena or other CRI-licensed IP providers; no need for customers to negotiate a separate DPA patent license with CRI for any IP running on S class PolarFire FPGAs

Availability
Microsemi's PolarFire "S class" FPGAs with Athena's TeraFire cryptographic microprocessor will be available towards the end of the second quarter of 2017. In addition, a soft version of this core is available for Microsemi's SmartFusion2 SoC FPGAs. For more information, visit [www.microsemi.com/polarfire](http://www.microsemi.com/polarfire) or email sales.support@microsemi.com.

About PolarFire FPGAs
Microsemi's new cost-optimized PolarFire FPGAs deliver the industry's lowest power at mid-range densities with exceptional security and reliability. The product family features 12.7 Gbps Serializer/Deserializer (SerDes) transceivers at up to 50 percent lower power than competing FPGAs. Densities span from 100K to 500K logic elements (LEs) and are ideal for a wide range of applications within wireline access networks and cellular infrastructure, defense and commercial aviation markets, as well as industry 4.0 which includes the industrial automation and Internet of Things (IoT) markets.

PolarFire FPGAs' transceivers can support multiple serial protocols, making the products ideal for communications applications with 10Gbps Ethernet, CPRI, JESD204B, Interlaken and PCIe. In addition, the ability to implement serial gigabit Ethernet (SGMII) on general purpose input/output (GPIO) enables numerous 1Gbps Ethernet links to be supported. PolarFire FPGAs also contain the most hardened security intellectual property (IP) to protect customer designs, data and supply chain. The non-volatile PolarFire product family consumes 10 times less static power than competitive devices and features an even lower standby power referred to as Flash*Freeze. For more information, visit [www.microsemi.com/polarfire](http://www.microsemi.com/polarfire).

About Microsemi's Security Solutions Portfolio
Microsemi is a leading provider of information assurance (IA) and anti-tamper (AT) solutions and services to U.S. federal organizations, systems integrators and industries requiring a high level of electronic security including financial, digital rights management, gaming, industrial automation and medical. The company leverages its proven hardware and software IA/AT technologies, innovative cryptographically-secure supply chain risk management process and extensive industry experience to secure critical program information and technology through the entire system lifecycle. In addition, Microsemi provides secure synchronous time generating systems, secured Ethernet connectivity, controller-based data encryption for data protection and security solutions in data centers, comprehensive IA/AT services such as risk assessments, protection development and red teaming to satisfy security requirements. For more information on Microsemi's security products and technologies, visit [http://www.microsemi.com/design-support/security-technology](http://www.microsemi.com/design-support/security-technology) and for more information on Microsemi's product portfolio, visit [http://www.microsemi.com/products/](http://www.microsemi.com/products/).

About Microsemi
Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California, and has approximately 4,800 employees globally. Learn more at [www.microsemi.com](http://www.microsemi.com).
About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit athena-group.com.

The Licensed DPA Logo and the Security Logo are trademarks or registered trademarks of Cryptography Research, Inc. in the United States and other countries, used under license.

Microsemi and the Microsemi logo are registered trademarks or service marks of Microsemi Corporation and/or its affiliates. Third-party trademarks and service marks mentioned herein are the property of their respective owners.

"Safe Harbor" Statement under the Private Securities Litigation Reform Act of 1995: Any statements set forth in this news release that are not entirely historical and factual in nature, including without limitation statements related to Microsemi and The Athena Group, Inc. announcing Athena's TeraFire-hardened cryptographic microprocessor is included in Microsemi's new PolarFire field programmable gate array (FPGA) "S class" family members, and its potential effects on future business, are forward-looking statements. These forward-looking statements are based on our current expectations and are inherently subject to risks and uncertainties that could cause actual results to differ materially from those expressed in the forward-looking statements. The potential risks and uncertainties include, but are not limited to, such factors as rapidly changing technology and product obsolescence, potential cost increases, variations in customer order preferences, weakness or competitive pricing environment of the marketplace, uncertain demand for and acceptance of the company's products, adverse circumstances in any of our end markets, results of in-process or planned development or marketing and promotional campaigns, difficulties foreseeing future demand, potential non-realization of expected orders or non-realization of backlog, product returns, product liability, and other potential unexpected business and economic conditions or adverse changes in current or expected industry conditions, difficulties and costs in implementing the company's acquisitions and divestitures strategy or integrating acquired companies, uncertainty as to the future profitability of acquired businesses and realization of accretion from acquisition transactions, difficulties and costs of protecting patents and other proprietary rights, inventory obsolescence and difficulties regarding customer qualification of products. In addition to these factors and any other factors mentioned elsewhere in this news release, the reader should refer as well to the factors, uncertainties or risks identified in the company's most recent Form 10-K and all subsequent Form 10-Q reports filed by Microsemi with the SEC. Additional risk factors may be identified from time to time in Microsemi's future filings. The forward-looking statements included in this release speak only as of the date hereof, and Microsemi does not undertake any obligation to update these forward-looking statements to reflect subsequent events or circumstances.

SOURCE Microsemi Corporation and The Athena Group, Inc.

For further information: Microsemi Corp., Farhad Mafie, VP Worldwide Product Marketing, 949-380-6161, press@microsemi.com; The Athena Group, Inc., Pat Rugg, 407-278-5850, pat.rugg@athena-group.com

Additional assets available online: Photos (1)