

Microsemi and INVIA First to Deliver DPA-resistant Cryptographic Software on SmartFusion®

Solution Provides Enhanced Protection for Security Applications

ALISO VIEJO, Calif., Dec. 19, 2011 --**Microsemi Corporation (Nasdaq: MSCC)**, a leading provider of semiconductor solutions differentiated by power, security, reliability and performance, today announced the immediate availability of INVIA's differential power analysis (DPA)-resistant products on Microsemi's flash-based FPGA devices and [SmartFusion®](#), the industry's only customizable system-on-chip (cSoC) solution which integrates an FPGA with analog functions and a hard ARM microcontroller core. DPA is a technique used by hackers to extract secret keys and compromise the security of semiconductors and tamper-resistant devices by analyzing their power consumption. Microsemi is the only major provider of cSoCs and FPGAs to hold a patent license from Cryptography Research, Inc (CRI) for DPA-countermeasures, and to offer INVIA's software libraries for AES, RSA and ECC cryptographic algorithms.

"Our collaboration with INVIA provides our customers with leading-edge solutions that guard against the increasingly serious threat of DPA security breaches in government, industrial, financial and other high-profile applications," said Esam Elashmawi, vice president and general manager at Microsemi. "Combined with our ability to pass through Microsemi's CRI license to customers for many products, this allows them to employ DPA countermeasures quickly and efficiently-truly maximizing our relationships for the benefit of our customer base."

INVIA's DPA- and fault-resistant cryptographic library runs on Microsemi's SmartFusion single-chip cSoC, which features a Cortex™-M3 MCU, a full-fledged FPGA and analog circuits all on a single-chip. Available immediately are INVIA's DPA-resistant implementations of the popular AES private key, RSA public key algorithms and ECC public key algorithm.

"We're pleased that through our partnership with Microsemi, we're able to deliver customers crypto-algorithms designed to resist the most advanced side-channel and fault-injection attacks," said Martin Gallezot, marketing and sales director of INVIA. "Software with this level of security used to be available only on smart card-like devices. It is now available on SmartFusion devices."

For more information on Microsemi's SoC products visit: www.microsemi.com/soc. Those interested in licensing INVIA's AES, RSA, or ECC software libraries should contact Gallezot at martin.gallezot@invia.fr or +33-44-22-45070.

About Microsemi

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative

energy markets. Products include high-performance, high-reliability analog and RF devices, mixed-signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,000 employees globally. Learn more at www.microsemi.com.

About INVIA

INVIA is a privately held company founded in 2006 by smart card industry veterans. INVIA provides security related design IP to ASIC & FPGA designers. INVIA products protect silicon designs against tampering, reverse engineering, cloning and other major security threats. INVIA also provides embedded software cryptography for ARM Cortex and SPARC processors. INVIA's IPs are used in millions of field-proven devices. Our R&D's experience in secure hardware and software exceeds 150 men years and is protected by a patent portfolio. For press inquiries, please contact Martin Gallezot at +33 442 245 084 or martin.gallezot@invia.fr.

###

Microsemi and the Microsemi logo and all other marks used herein are registered trademarks or service marks of Microsemi Corporation and/or its affiliates; except that 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 the availability of INVIA's differential power analysis (DPA)-resistant products on its SmartFusion[®] customizable system-on-chip (cSoC), and their 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 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.