eWBM Achieves First-Pass Silicon Success for Highly Secure Microcontroller with Synopsys Security IP

High-Quality DesignWare Security IP Delivers Functionality Required to Protect Against Threats in IoT Applications

MOUNTAIN VIEW, Calif., Aug. 18, 2016 /PRNewswire/ --

Highlights:

- eWBM's MS1000 microcontroller with embedded security in volume production and certified for FIDO universal two-factor authentication
- DesignWare tRoot Hardware Root of Trust enables implementation of Trusted Execution Environments for protecting sensitive information and data processing
- DesignWare True Random Number Generators provide standards-compliant, cryptography quality random numbers
- DesignWare Security Protocol Accelerators increase performance and enable processor offload for cryptographic operations and security protocols

Synopsys, Inc. (Nasdaq:SNPS) today announced that eWBM achieved first-pass silicon success for its MS1000 microcontroller with embedded security using Synopsys' DesignWare® tRoot™ Secure Hardware Root of Trust, True Random Number Generator (TRNG), and Security Protocol Accelerator IP. The IP enables the implementation of a wide range of hardware-enforced security functions that help protect IoT devices against evolving threats and secure sensitive data such as encryption keys and identity credentials. By using standards-compliant DesignWare Security IP, eWBM achieved Fast IDentity Online (FIDO) universal two-factor (U2F) certification for its MS1000 microcontroller, demonstrating a robust single-chip solution that protects data from external attacks without requiring peripheral components.

"With the increase in IoT security breaches, we needed to collaborate with a proven IP provider to deliver a microcontroller with superior security capabilities," said Stephen Oh, CEO at eWBM. "Synopsys was the only provider offering a comprehensive portfolio of security IP solutions that enabled us to implement the required hardware-based security features. The DesignWare IP took only days to integrate and enabled us to deliver a robust, certified security microcontroller on schedule. Due to our success using the DesignWare IP, we immediately chose Synopsys for our new MS500/MS300 microcontrollers, and we expect the high-quality, widely deployed DesignWare IP to continue to meet our design needs."

The MS1000 microcontroller integrates a combination of DesignWare Security IP to perform secure boot, secure authentication, real-time integrity monitoring, secure storage for management of keys and other sensitive information, and hardware acceleration. The DesignWare tRoot Secure Hardware Root of Trust provides the security functions for Trusted Execution Environments, which enable connected devices to securely start up, identify, authenticate and communicate. The DesignWare TRNG provides standards-compliant, high-quality true random numbers that are crucial elements for security standards and protocols. The TRNG is fully digital and combines a whitening circuit with a noise source that provides automatic seeding of the random number stream. The configurable DesignWare Security Protocol Accelerator (SPAcc) reduces bus traffic and offers increased throughput by supporting efficient data sequencing as well as parallel processing of encryption and hashing cryptographic operations.

"Security is fundamental to the growth of the IoT, and incorporating security at the lowest levels of the SoC design helps protect devices through their lifecycles," said John Koeter, vice president of marketing for IP and prototyping at Synopsys. "Synopsys delivers a broad range of security IP solutions, including the tRoot Secure Hardware Root of Trust, TRNGs and SPAccs, which enable companies such as eWBM to create highly secure systems that protect connected devices from evolving threats."

Availability & Resources

The DesignWare tRoot Secure Hardware Root of Trust, True Random Number Generator (TRNG), and Security Protocol Accelerator (SPAcc) are available now.

- Learn more about DesignWare Security IP
- Download the eWBM success story
- View the webinar: "Securing IoT Systems with a Root of Trust"
- Read the white paper: True Random Number Generators for Truly Secure Systems

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio

includes logic libraries, embedded memories, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP prototyping kits, IP software development kits and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enable designers to reduce integration risk and accelerate time-to-market. For more information on DesignWare IP, visit https://www.synopsys.com/designware.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software quality and security solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest quality and security, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at https://www.synopsys.com/.

Editorial Contacts:
Monica Marmie
Synopsys, Inc.
650-584-2890
monical@synopsys.com

SOURCE Synopsys, Inc.