Synopsys Accelerates FIPS 140-2 Certification with NIST-Validated Cryptography IP Software Library

Successful Testing of DesignWare Cryptography Software Library Enables Development of Highly Secure IoT Systems

MOUNTAIN VIEW, Calif., Nov. 1, 2017 /PRNewswire/ --

Highlights:

- DesignWare Cryptography Software Library includes a suite of widely used encryption and certificate processing functions required for embedded applications
- Secure functions that passed validation tests include block ciphers, digital signatures, secure hashing (SHA-3) and random number generators, reducing design risk for SoCs requiring high levels of security
- DesignWare Cryptography Software Library is available for DesignWare ARC EM, ARC HS, ARM and x86 processor platforms

Synopsys, Inc. (Nasdaq: SNPS) today announced it has successfully validated the DesignWare® Cryptography Software Library through the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP). To earn validation, the DesignWare Cryptography Software Library passed a full suite of validation tests for secure functions including block ciphers (AES, DES), digital signatures (RSA and ECC based), secure hashing (SHA-1, 2 and 3) and random number generation. By providing cryptography software that has been extensively tested and validated through the NIST CAVP, Synopsys enables designers to accelerate Cryptographic Module Validation Program (CMVP) and Federal Information Processing Standard (FIPS) 140-2 certification for applications requiring high levels of security.

The DesignWare Cryptography Software Library features the most widely used symmetric and asymmetric cryptography algorithms in a wide range of size and performance configuration options including hardware offload. For applications that will be ported to multiple platforms, the DesignWare Cryptography Software Library supports DesignWare ARC®, ARM® and x86 processor platforms and build environments including Linux, Android, Apple iOS and Microsoft Windows operating systems.

"The need for increased cybersecurity has been recognized industrywide, requiring advanced security solutions to protect against growing vulnerabilities," said John Koeter, vice president of marketing for IP at Synopsys. "Security needs to be addressed at all levels, from the SoC to the software applications. By using DesignWare Cryptography Software Libraries that have been validated by NIST CAVP, designers can be confident that the functions will operate as expected to help them meet the most stringent FIPS certification criteria for their application."

Availability & Resources

The DesignWare Cryptography Software Library and Cryptography IP are available now.

- View DesignWare Cryptography Software Library validation on the NIST.gov website
- Learn more about NIST CAVP validation: Ensure Robust Encryption with CAVP Validation for FIPS 140-2 Conformance

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 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 www.synopsys.com.

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

SOURCE Synopsys, Inc.

Additional assets available online: