NXP LPC55S16 MCU Awarded PSA Level 2 and SESIP Assurance Level 2 Certifications

November 17, 2020

EINDHOVEN, The Netherlands, Nov. 17, 2020 – NXP Semiconductors N.V. (NASDAQ: NXPI) announced the LPC55S16 MCU has been awarded Level 2 certifications by both the PSA Certified scheme co-developed by Arm and the GlobalPlatform Security Evaluation Standard for IoT Platforms (SESIP) using the secure protection profile for embedded processors. With fast-expanding IoT and Industrial edge applications, device security and data protection become paramount. These certifications provide validation of NXP's security-by-design approach and further enhance OEMs and consumer confidence in NXP enabled edge devices.

Part of the NXP EdgeVerse™ computing and security portfolio, the LPC55S16 MCU is a member of the general purpose LPC5500 MCU series based on the Arm® Cortex®-M33 core. This series offers performance efficiency leveraging 40-nm NVM process technology, advanced security, and mixed-signal capabilities.

Both the SESIP and PSA Certified testing and certifications were done by Brightsight, one of the best-known independent security evaluation laboratories.
The LPC55S16 MCU achieved PSA Certified Level 2 that is based on a comprehensive assurance framework to showcase robustness of the security, enabling device manufacturers to reduce additional security testing and improve time to market. It uses a 25-day time-boxed laboratory evaluation against the PSA Root of Trust (PSA-RoT) security claims to demonstrate that the device can protect against scalable software attacks.
To achieve GlobalPlatform SESIP 2, the LPC55S16 MCU underwent source code analysis and penetration testing issued by Brightsight and was validated by another independent certification body. SESIP certification helps assure product security claims are tested and verified, and provides evidence of the LPC55S16 MCU's resistance to basic attack potential. SESIP allows for customers to re-use the LPC55S16 MCU validation results in the certification process for their end applications.
The LPC55S16 MCU integrated security features include:

- Arm TrustZone® technology, which enables system-wide software protection with the ability to securely isolate peripherals to reduce the risk of attack on critical components
- AES-256 accelerator provides confidentiality and secure hash algorithm (SHA2) accelerator provides integrity of secure communications and secure boot
- PRINCE module offers real-time encryption and decryption of the on-chip flash to provide both secure storage of data and asset protection of software intellectual property (IP)
- CASPER Crypto co-processor enables hardware acceleration of various asymmetric cryptographic algorithms to establish secure connections
- Physical Unclonable Function (PUF) uses dedicated on-chip SRAM to construct unique device root keys (64 to 4096 bits) for secure storage
- 128-bit unique device serial number for identification (UUID)
- True Random Number Generator (TRNG)
- Code watchdog enables integrity checking of execution flow of the firmware
- Debug authentication protocol for secure debugging

Certified EdgeLock™ Assurance
The LPC55S16 MCU is part of the Certified EdgeLock Assurance program. Designed to meet industry standards, NXP products and services in the EdgeLock Assurance program follow proven security development processes and verification assessments – from product concept through release – to help ensure customers receive trusted solutions for their security challenges.

Product Availability
The LPC55S16 MCU family is available now with a suggested resale price starting at $1.54 (USD) for 10,000-unit quantities.

Visit the LPC55S16 MCU for more information.

Also see EdgeLock Assurance, PSA Certified, and Security Evaluation Standard for IoT Platforms (SESIP) published by GlobalPlatform web pages for further details.

About NXP Semiconductors
NXP Semiconductors N.V. enables secure connections for a smarter world, advancing solutions that make lives easier, better, and safer. As the world leader in secure connectivity solutions for embedded applications, NXP is driving innovation in the automotive, industrial & IoT, mobile, and communication infrastructure markets. Built on more than 60 years of combined experience and expertise, the company has approximately 29,000 employees in more than 30 countries and posted revenue of $8.88 billion in 2019. Find out more at www.nxp.com.

###

For more information, please contact:

Americas & Europe	**Greater China / Asia**
Jason Deal	Ming Yue
Tel: +44 7715228414	Tel: +86 21 2205 2690
Email: jason.deal@nxp.com	Email: ming.yue@nxp.com