New NXP Microcontrollers Deter Security Threats to Application Code and Data in Connected Applications

February 24, 2015 3:00 AM ET

High-Performance LPC18Sxx and LPC43Sxx Microcontroller Families Add Hardware-Accelerated Encryption for Secure Boot and Secure Messaging

EINDHOVEN, Netherlands and SAN JOSE, Calif., Feb. 24, 2015 (GLOBE NEWSWIRE) -- NXP Semiconductors N.V. (Nasdaq:NXPI) today announced two new microcontroller families, LPC18Sxx and LPC43Sxx, to help embedded developers secure application code and data messages in connected applications against threats such as theft and cloning. The new microcontroller families add support for secure boot and secure messaging to the long list of advanced control, high-speed connectivity, display, advanced timing, and flexible peripheral features for which the popular LPC1800 and LPC4300 series are known.

The LPC18Sxx and LPC43Sxx microcontroller families are well suited for any 'connected' application, particularly hubs or gateways, tasked with relaying and/or bridging large volumes of high-speed data. These functions are common in products such as smart meter communications hubs, factory, building, and home automation devices, streaming audio products, automotive aftermarket and many more.

"The tremendous growth in 'connected things' has begun and will accelerate exponentially in the coming years," said Ross Bannatyne, general manager, mass market product line, microcontroller business line, NXP Semiconductors. "With increased connectivity comes risk, and developers now need to understand and defend against threats to the code and data messages. The new LPC18S and LPC43S microcontroller families help embedded developers protect connected applications from these threats, whether they are used standalone, with security solutions from software partners, or paired with an NXP A-Series secure element."

"The Internet of Things (IoT) must be built from the ground up with security in mind," said Tom Mudryk, technical director, ESL Smart Solutions, Ltd. "Working with NXP and Cypherbridge, we have created a secure IoT solution that offers our customers a valuable yet convenient service, whilst maintaining data security and integrity. We selected NXP's LPC1800 series for our gateway product because of its vast connectivity options and integrated LCD driver, and of course the new integrated security features provide that extra layer of protection."

A spectrum of solutions for secure connectivity

Both LPC18Sxx and LPC43Sxx families integrate an AES-128 encryption engine for fast, secure bulk message transfers; two 128-bit non-volatile OTP memories for encrypted, hardware-randomized key storage to prevent cloning; a true random number generator for unique key creation; and boot ROM drivers supporting secure boot of authenticated encrypted firmware images. The MCUs in both families use high-performance Cortex-M cores (Cortex-M3/LPC18Sxx, LPC43Sxx/Cortex-M4 & M0) ensuring ample bandwidth for fast bulk data encryption or decryption without slowing down communications. They also include code read protection (CRP) to prevent unauthorized access to internal Flash.

The LPC43Sxx and LPC18Sxx microcontroller families anchor a spectrum of secure connectivity solutions from NXP. Both families are supported by software solutions from ecosystem partners for secure firmware updates, secure IoT connectivity, and secure networking stacks (SSL, TLS). In addition these new MCUs can be seamlessly paired with an NXP A-Series secure element for a turnkey solution to add tamper detection, secure authentication with hardware-accelerated PKI (RSA and ECC keys), secure certificate storage and more.

Like all LPC microcontrollers, the new LPC43Sxx and LPC18Sxx microcontroller families are fully supported by the LPC developers' ecosystem. This provides an extensive collection of tools, drivers and middleware, as well as popular forums in constant use by a highly engaged community of embedded developers. To enable developers to bring secure, connected products to market quickly, LPCXpresso evaluation boards are available for both families. Each includes an LPC MCU and NXP A7001CM secure element as well as numerous connectivity and development/debugging interfaces. Together

with the LPCXpresso IDE or third-party tool-chain support, plus free LPCOpen drivers and example code, these boards provide a complete low-cost evaluation/development platform.

An LPC43S37-based development platform, available in Q2, will help designers implement a range of secure connectivity solutions for IoT, Industry 4.0, consumer and other applications. The platform combines the MCU, security software from ecosystem partners, an NXP A-Series secure element and supports connectivity features including Ethernet and WiFi.

Availability and demonstration

Parts in both MCU families will be available in multiple sizes of LQFP and BGA packages.

They are available now with pricing starting at USD $3 in 4K quantities. The LPCXpresso18S37 and LPCXPresso43S37 evaluation boards are available now through NXP-authorized distributors.

The LPC18Sxx and LPC43Sxx microcontroller families will be demonstrated in the NXP booth #5-378, in hall 5 at embedded world 2015 in Nuremberg, February 24 – 26.

Additional product information is available online:

- LPC18Sxx Family Microcontrollers
- LPC43Sxx Family Microcontrollers
- NXP A7001 Secure Element
- LPCXpresso18S37 evaluation board
- LPCXpresso43S37 evaluation board

About NXP Semiconductors

NXP Semiconductors N.V. (Nasdaq:NXPI) creates solutions that enable Secure Connections for a Smarter World. Building on its expertise in High Performance Mixed Signal electronics, NXP is driving innovation in the application areas Connected Car, Security, Portable & Wearable and Internet of Things. NXP has operations in more than 25 countries, and posted revenue of $5.65 billion in 2014. Find out more at nxp.com.

Forward-looking Statements

This document includes forward-looking statements which include statements regarding NXP's business strategy, financial condition, results of operations and market data, as well as other statements that are not historical facts. By their nature, forward-looking statements are subject to numerous factors, risks and uncertainties that could cause actual outcomes and results to be materially different from those projected. Readers are cautioned not to place undue reliance on these forward-looking statements. Except for any ongoing obligation to disclose material information as required by the United States federal securities laws, NXP does not have any intention or obligation to publicly update or revise any forward-looking statements after NXP distributes this document, whether to reflect any future events or circumstances or otherwise. For a discussion of potential risks and uncertainties, please refer to the risk factors listed in NXP's SEC filings. Copies of NXP's SEC filings are available from the SEC website, www.sec.gov.

CONTACT: For further press information, please contact:
NXP Semiconductors
Europe: Martijn van der Linden
+31 6 10914896
martijn.van.der.linden@nxp.com

Greater China / Asia: Esther Chang
+886 2 8170 9990
esther.chang@nxp.com

Americas: Hillary Cain
+1 408 518 5227
hillary.cain@nxp.com

NXP
Semiconductors

NXP Semiconductors