Entrust provisions root identity for Microchip's IoT-ready SAM L11 Microcontrollers

The Internet of Things (IoT) has become an unstoppable phenomenon. Although viewed by many as a highly conservative number, IDC predicts that the total number of connected IoT devices will exceed 40 billion by 2025.

However, the explosive proliferation of IoT-related endpoints – ranging from autonomous vehicles to smart household appliances, and healthcare equipment to agricultural machinery – is not without its own challenges. Among the most critical of these is the issue of security – ensuring that every device is protected against compromise.

BUSINESS NEED

Anand Rangarajan, product marketing manager for Microchip Technology, elaborated, "The IoT universe currently has no pervasive standards for security. The sheer complexity of incorporating appropriate security measures into their products is a daunting proposition for many manufacturers."

> **Integrating industrial-strength security into an embedded system is a real game-changer for the whole IoT marketplace.**
>
> – Anand Rangarajan, product marketing manager for Microchip Technology

LEARN MORE AT ENTRUST.COM/HSM

Microchip

Renowned for its continuous innovation and precedent-setting products, Microchip Technology, Inc. is one of the world's leading providers of microcontroller, mixed-signal, analog and flash-IP solutions. One of the company's latest microcontrollers, the SAM L11, awarded the 2018 Innovation Award for Best Contribution to IoT Security at ARM Techcon, specifically addresses the feature, functionality and security needs of IoT nodes and smart endpoints, such as medical devices, sensors, cameras and cars.

Headquartered in Chandler, Arizona, Microchip is publicly traded on the Nasdaq exchange. The company has shipped billions of microcontrollers and microprocessors to hundreds of thousands of customers around the world.

TECHNOLOGY NEED

"From a microcontroller perspective, the type of use case we anticipate for the SAM L11 dictates some very unique design characteristics, like the need for high performance but low power consumption," described Rangarajan.

SOLUTION

At the heart of the SAM L11's security architecture is a root of trust function created by Microchip to enable a device-unique key to be inserted during manufacture. Choosing the technology to manage and execute the critical task proved to be very straightforward. "We've had a long-standing relationship with Entrust (previously nCipher) and selecting their hardware security module (HSM) to generate the individual keys was a clear-cut choice for us," noted Rangarajan.

The Entrust nShield® HSM is a certified hardware security appliance that executes critical encryption, digital signing and key generation functions. The hardened networked platform is highly scalable, and utilizes a uniquely flexible architecture that is capable of industry-leading cryptographic transaction rates.

RESULTS

"Having the ability to insert a unique key from the nShield HSM into each SAM L11 microcontroller enables devices to be individually identified, verified and managed remotely. This is particularly important when trust needs to be re-established between IoT devices and other connected endpoints," Rangarajan observed. "Manufacturers can now take full advantage of the cloud to provide secure, pervasive connectivity between each node. It's ideal for applications like securing wireless sensors, encrypting data from handheld medical devices and even remote authentication of cloud-connected systems."

Part of the Microchip SAM L11 microcontroller's very compelling value proposition is the result of the company's partnership with Trustonic, a leader in the device security market with over 1.5 billion protected units deployed worldwide.

One of the biggest breakthroughs has been Trustonic's creation of a library of security functions – including authentication, secure boot, tamper detection, AES and SHA encryption, and secure key storage – that is incorporated into a software development kit.

Microchip

> **Selecting the Entrust nShield HSM to generate the individual keys was a clear-cut choice for us.**
>
> – Anand Rangarajan, product marketing manager for Microchip Technology

"Designers can now use the modular security framework to make simple API calls to access the very sophisticated set of security capabilities we've built," commented Rangarajan. "An in-depth expertise with chip-level protocols is no longer needed. This greatly accelerates development timeframes and dramatically reduces the overhead traditionally associated with securing an IoT device."

The library of security modules is built on top of Kinibi-M, a modular, hardware-secured operating environment custom designed by Trustonic for size-constrained IoT chipsets. Underneath Kinibi-M, a hardware abstraction layer facilitates direct communication with the SAM L11, including managing the use of the encrypted Entrust nShield-generated key.

"The Microchip developers of the SAM L11 did their own due-diligence to determine that the Entrust nShield HSM was the optimal choice for us, but quite separately, Trustonic also recommended that we should use the Entrust HSM. It was very validating to get a completely independent endorsement of our decision," recalled Rangarajan.

SIMPLIFYING SECURITY WITH A GAME-CHANGING CHIP

The SAM L11 is the first microcontroller in the industry to utilize the Arm Cortex-M23 processor and Arm TrustZone embedded security technology; providing hardware-enforced isolation between trusted and untrusted resources. Rangarajan reflected, "Despite the sophistication and comprehensive capabilities of the security architecture, using Kinibi-M still makes secure application development simpler with a firmware that is fully integrated with SAM L11's security features, and offers code examples to address relevant IoT use cases that could benefit from a device like SAM L11."

The ability to provide IoT device developers with a world-class root-of-trust foundation by utilizing keys generated by an Entrust nShield® HSM is having a significant global impact. Rangarajan stated, "The approach we've taken means we're now able to incorporate security into a high-performance package that has extremely low power consumption. Integrating industrial-strength security into an embedded system is a real game-changer for the whole IoT marketplace."

Microchip

TRANSFORMING SECURITY ACROSS THE IoT

Business need

- Create solution to secure IoT nodes and endpoints
- Cut complexity and cost of incorporating security into IoT devices
- Remove need for specialized chip-level programming skills

Technology need

- Integrate robust security features into fast, power-efficient microcontroller
- Design small footprint to enable use with memory-intensive applications
- Establish root of trust

Solution

- Entrust nShield HSM

Result

- Release of SAM L11 microcontroller with industry-leading features and performance
- Software development kit delivers simple API access to sophisticated security functions
- Reduced time-to-market for IoT device manufacturers
- Enables trust for IoT devices and the data they produce

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com

Entrust is a trademark, registered trademark, and/or service mark of Entrust Corporation in the United States and/or other countries. ©2020 Entrust Corporation.