# Micron Addresses IoT Security with New Authenta™ Technology in Flash Memory

-By Jeff Shiner, Marketing Director, IoT Solutions, Micron

Only a couple of years ago we were discussing how one day the Internet of Things (IoT) would enable higher levels of intelligence and functionality in an array of things, from devices in the home to the factory. This growth is happening faster than many expected, but so are the cyber-attacks that are leveraging these connected devices everywhere. According to Gartner, by 2020, over 25% of identified attacks in enterprises will involve IoT. So far, the cost and complexity of adding security to IoT end-points has led to it mostly being ignored or an afterthought. But continued onslaught of cyber-attacks has raised the awareness that OEMs can no longer afford to ignore this issue and risk their IoT driven business and company's reputation. They must embed security in the DNA of their IoT devices now.

To address this challenge, Micron has launched a new technology capability that adds a strong layer of defense to a broad array of IoT devices. This technology can build upon existing levels of security as defense in depth layered security where previously it may have been too costly. The premise is simple: We're leveraging existing standard non-volatile memory (NVM) sockets, or flash memory, to do heavy-lifting that protects the integrity of the device itself and the software that runs on the device. New Micron® flash memory with Authenta™ technology will replace existing flash devices with the same NVM function while adding a new unique level of hardware-based security capabilities.  System designers can leverage these capabilities into an end-to-end, cloud-to-device IoT security strategy enabled by simple middleware and software development kits (SDKs).

## A Zero-Component Approach: Just Use Flash

Flash memory has been one of the most standardized semiconductors in electronic devices since early PC days. That's when the Basic Input/Output System (BIOS) was one of the first solutions to leverage a single volt power supply flash memory that could provide nonvolatility and the ability to make in-system modifications. Over time as more functionality and performance have been added to flash memory, the electrical interface to flash has remained fairly constant. Various types of flash memory exist today, including serial NOR, parallel NOR, serial NAND, parallel NAND, e.MMC, UFS, etc. These sockets are source-able from multiple vendors and are used in most embedded systems across various industries and applications.

For example, today we see standard serial NOR in an array of applications like medical devices, factory automation boards, automotive ECUs, smart meters and internet gateways, just to name a few. Given diversity of chipset architectures (processors, controllers or SoCs), operating systems, supply chains used across these applications, flash memory represents the most common denominator building block in these systems. Leveraging flash memory to add a strong level of security capability in the system makes this approach possibly the simplest and most scalable security implementation in the industry.

## Location of Your Hardware-Based Roots of Trust Matters

System resilience today is typically characterized by the location of "roots of trust" integrated into devices and leveraged by the solution for the security functions they provide. For more information on roots of trust, look for the definition created by the National Institute of Technology (NIST) in Special Publication 800-164. The industry has lot of varied implementations of roots of trust at the system level, using a mix of hardware and software capabilities, resulting in fragmentation of approaches and confusing level of security. The perplexing array of options has also done a good job of masking a key gap: how to defend the non-volatile memory which is where critical code and data is stored.

Standard thinking is driving engineers to expect the processor and other secure elements like hardware security modules (HSMs) to offer critical security services to their systems. This has created a security gap at the lowest levels of boot in many systems where discrete flash memory components store system-critical code and data. The flash has become the target for many hackers to create Advanced Persistent Threats (APT's) that can mask themselves from higher levels of code and resist removal. In many of these cases, flash memory is re-imaged or rewritten with new malicious code undermining the integrity of that device.

Micron's Authenta™ technology integrates true hardware-based roots of trust into flash memory, enabling strong cryptographic identity and health management for IoT devices. By moving essential security primitives in-memory, it becomes simpler to protect the integrity of code and data housed within the memory itself. This approach significantly enhances system level security while minimizing the complexity and cost of implementations.

## Making Security Easy to Implement

Micron and Microsoft announced a new IoT device management capability that leverages key elements of the new Authenta technology in flash memory. This capability enables device onboarding and management by the Microsoft® Azure® IoT cloud using Micron's Authenta enabled flash memory and associated software solutions. The Micron solutions offer a strong cryptographic identity that becomes the basis for critical device provisioning services like the newly announced Azure IoT Hub Device Provisioning Service (DPS). This new DPS along with Authenta enabled memory can enable zero-touch provisioning of devices to the correct IoT hub and other valuable services.

To implement this capability, Micron and Microsoft leveraged the Device Identity Composition Engine (DICE), an upcoming standard from the Trusted Computing Group (TCG), and Micron's Authenta enabled memory to demonstrate how only trusted hardware can gain access to the Microsoft Azure IoT cloud. One key aspect of the combined solution is that the health and identity of an IoT device is verified in memory where critical code is typically stored. The unique DNA of each IoT device can now offer customers end-to-end device integrity at a new level, starting at the boot process. This will enable additional functionality like hardware-based device attestation and provisioning and administrative remediation of the device if necessary.

## Strong Identity and Security for All

Today, it is expected that Fortune 100 companies staff cybersecurity specialists with the intent to provide world-class cybersecurity protection at all levels possible. This comes at a high cost, and smaller companies don't have the options that larger companies must offer these corporate services. The cost of hardware and software security implementation and management, and the significant fragmentation of security technology, have created too many hurdles for many companies to burden. With the release of the Authenta technology, Micron, in collaboration with partners, intends to simplify device security implementations and significantly reduce financial burdens for all companies to launch IoT deployments affordably and securely.

**Online**
www.arrow.com/IoT

Five Years Out