Everyday products are being connected, with intelligence being integrated into almost all aspects of our lives. Experts agree this paradigm shift has created unique issues surrounding security, which leaves consumers and companies vulnerable to a myriad of cyberattacks.

With network boundaries becoming more scattered, protecting network architecture is no longer enough. Companies must also protect against vulnerabilities and threats that exist inside and outside of their previous trusted networks.

Micron’s Authenta™ Technology

While companies are looking to secure their devices, they’re facing a number of issues in doing so. Many firms lack the security architecture expertise to adequately design and build a secure solution, or even understand all options. They also tend to lack the resources to efficiently implement silicon-to-cloud solutions for secure connectivity.

Enter Authenta technology. Utilizing existing standard flash memory sockets in a wide range of Internet of Things (IoT) end-points, developers can strengthen system-level cybersecurity without the complexities of managing disperse SoC security architectures and cryptographic flows, and without additional hardware components. Micron’s Authenta technology provides a strong hardware-based protection for the lowest layers of IoT device software—starting with foundational device identities and the attestation of the lowest layer of boot process.

By combining device unique identity from the Authenta flash memory and its measurement capability necessary for in-memory secure boot, Authenta technology provides the ingredients for a strong dual-factor authentication of IoT devices directly with a host—whether in the cloud, at the edge, or on the device—leading to a more affordable and robust IoT solution.

Authenta technology protects the integrity of an IoT device by monitoring and safeguarding the software that runs on the device.
Features

**Cryptographic lock**
- A hardware-based mechanism that isolates and authenticates accesses to one or more blocks of flash memory
- Provides storage for logs, firmware images, credential digests; only modifiable by administrator
- Enables over-the-air (OTA) firmware updates (more flexible than one-time programmable arrays)

**Embedded 256-bit SHA2 measurement engine**
- Authenticates firmware images stored in flash—even before booting
- Produces HMAC digests of credentials entered by users, which can then be compared to a database

**HMAC-signed commands**
- Several HMAC-signed commands only succeed if the issuer has knowledge of the root key
- A monotonic counter prevents reusing the same signature twice
- Stateless host-endpoint interaction prevents falling in non-secure states

**Secure storage for secrets, including keys and hardware identity arrays**
- A symmetric server root key provides access control to a remote administrator
- A device unique secret for creation of Device Identifier Composition Engine (DICE) [2] hardware ID with RIoT used for communication authentication

Satisfying most security objectives for IoT devices does not require specialized and costly equipment. Micron’s Authenta technology devices have been designed for use with most existing systems that already include flash storage.

**Value for System OEMs**
- Leverages an SoC/MCU/MPU agnostic hardware root-of-trust that is available in devices—inside the NAND flash or NOR flash memory
- Provides simple integration and activation of the security function, as well as simple augmentation to existing security features for defense-in-depth
- Establishes trust and provenance early in the supply chain—as the chip is first deployed and securely loaded with IP and software content
- Provides unique device hardening features by creating added protection in the flash memory

**Value for Cloud Services and Cloud Platform Partners**
- The Authenta Key Management Service along with Authenta flash enables an Authenta security-as-a-service platform to activate the security functions in IoT devices, creating strong, dual-factor device identities that can be used for secure OTA, remote attestations, device onboarding, and lifecycle management of devices in the cloud
- The Authenta security-as-a-service business model is built for today’s market trend—revenue centered around the deployment of service rather than the shipment of hardware or software
- The Authenta platform can simply bring higher trust in IoT cloud services by enabling protection and trust in deployed devices

**Learn more**
For additional information on Micron’s Authenta technology and Authenta technology’s security architecture, visit [https://www.micron.com/products/advanced-solutions/authenta](https://www.micron.com/products/advanced-solutions/authenta) or contact us at [IoTSecurity@micron.com](mailto:IoTSecurity@micron.com).

---

Products are warranted only to meet Micron’s production data sheet specifications. Products, programs and specifications are subject to change without notice. No hardware, software or system can provide absolute security under all conditions. Micron assumes no liability for lost, stolen or corrupted data arising from the use of any Micron products, including those products that incorporate any of the mentioned security features. ©2019 Micron Technology, Inc. All rights reserved. All information herein is provided on an “AS IS” basis without warranties of any kind. Micron, the Micron logo and all other Micron trademarks are the property of Micron Technology, Inc. All other trademarks are the property of their respective owners. Rev. A 10/19 CMM004-97676390-11361