Micron® Authenta™ Technology

A New Level of Cyber Protection for IoT Devices

Micron Authenta™ technology provides a unique level of protection for the lowest layers of Internet of Things (IoT) device software—starting with the boot process. Utilizing existing standard flash memory sockets, developers can strengthen system-level cybersecurity without adding additional hardware components, leading to a more affordable and robust IoT solution. A wide range of IoT end-points and edge devices that use standard flash memory chips can now be enhanced for improved system-level cybersecurity, more pervasive zero-touch onboarding deployments and future device management capabilities.

Simple, Integrated, Secure

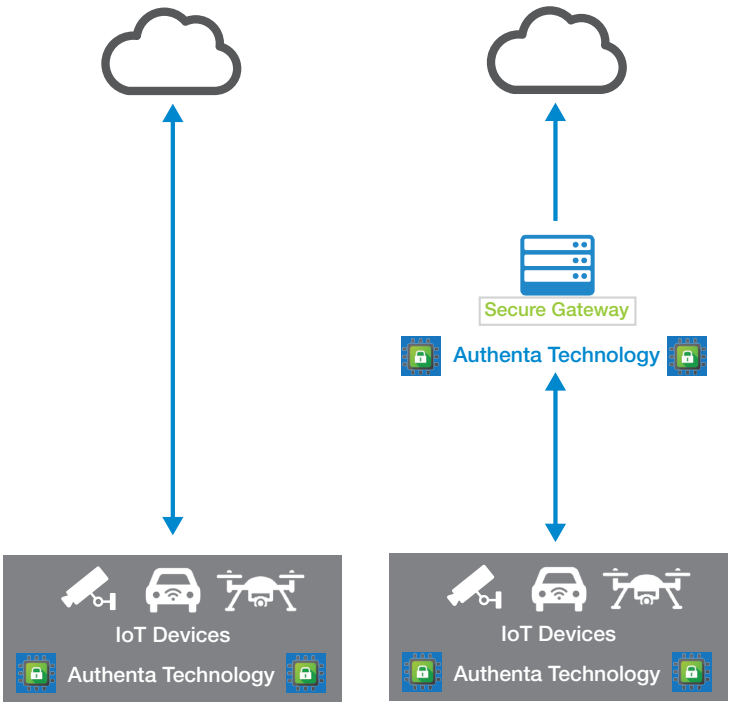
Micron's Authenta technology adds secure element features directly to flash memory to strengthen system-level security directly on the component that gives billions of IoT devices their identity.

By combining unique device-specific identity that only a hardware root of trust can provide, and the measurement capability necessary for in-memory secure boot, Authenta technology provides the ingredients necessary to authenticate IoT devices directly with a host—whether in the cloud, at the edge, or on the device. Authenta technology protects the integrity of the IoT device by monitoring and safeguarding the software that runs on the device.

Easy Device Management and Connectivity

In addition to the hardware, Micron offers software development kits (SDKs) that help make it easier to provide secure device management and connectivity for new platforms and devices, as well as the ability to retrofit legacy systems, offering fast time to market with lowered resources.

Authenta Technology Provides Simple Pervasive Protection and Identity



Security By Design
Built-in strong cryptographic identity simplifies secure device management—from supply chain to device onboarding through in-field updates and always-on firmware monitoring.

Zero-Component Solution
Security features built natively in flash memory enable advance system level-protection with hardware roots of trust, without adding any new hardware components.

Lower TCO for Security
Scalable solution for even the smallest embedded devices, lowers total cost to implement and manage first-class security and defense in-depth.

Learn more at micron.com

Contact us at IoTSecurity@micron.com

Authenta MPNs

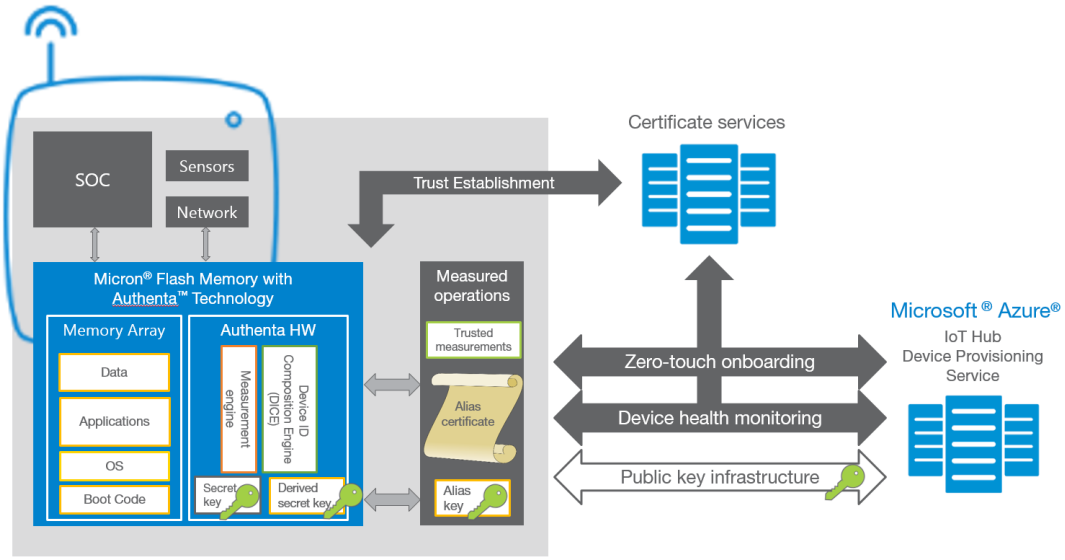
MT25QU128ABB1EW7-CAUT	MT25QU128ABB1EW7-CSIT
MT25QL128ABB1EW7-CAUT	MT25QL128ABB1EW7-CSIT

Micron® Authenta™ Technology

Simplifying End-to-End Security for IoT With Micron Authenta™ Technology and Microsoft® Azure®

Micron and Microsoft announce a new IoT device management capability that leverages key elements of Micron's new Authenta™ technology in flash memory. This capability enables device onboarding and management by the Microsoft® Azure® IoT cloud using Micron's Authenta-based flash memory and associated software solutions.

The Micron solution offers a strong cryptographic identity that becomes the basis for critical device provisioning services like the newly announced Azure Device Provisioning Service (DPS). This new DPS along with Authenta-enabled memory can facilitate zero-touch onboarding and provisioning of devices to the correct IoT hub, in addition to other valuable services.



Example of Micron's Authenta Technology Enabling Direct Connection to Microsoft Azure Cloud Services

How It Works

Leveraging the Device Identity Composition Engine (DICE), an upcoming standard from the Trusted Computing Group (TCG), Micron's Authenta-based memory demonstrates how only trusted IoT devices with healthy software can gain access to the Microsoft Azure IoT cloud platform.

One key aspect of the solution is the health and identity of an IoT device is verified in memory where critical code and data are typically stored. The unique DNA of each IoT device can offer customers end-to-end device integrity at a new level—starting at the boot process, where a cryptographic measurement is securely monitored by Microsoft's DPS that can then attest to the health of the firmware on IoT devices. This solution can also enable additional functionality such as administrative provisioning, remediation, and secure updates directly to the flash memory—simplifying device management deployments at the lowest cost to customers.

Making Security Easy to Implement with Strong Identity and Health

- Zero-component approach to billions of sockets
- Zero-touch device onboarding and provisioning
- Active device health monitor and detection
- Memory component-generated, code-specific certificates to verify with Azure IoT Hub
- Code measurement at the lowest levels of boot, infused with individual hardware identity
- Boot and runtime device malicious detection

Learn more at micron.com
Contact us at IoTSecurity@micron.com

Authenta MPNs

MT25QU128ABB1EW7-CAUT	MT25QU128ABB1EW7-CSIT
MT25QL128ABB1EW7-CAUT	MT25QL128ABB1EW7-CSIT