Micron® Authenta™ Key Management Service

Silicon-based Security-as-a-Service

Increasing Protection of the IoT

With the explosion of intelligent connected devices—from the home and automobile to industrial markets and enterprises—comes a problem: how to safely employ protection of these devices in a very diverse supply chain and fragmented ecosystem.

The opportunities for maliciously inserting malware, cloning or stealing valuable IP, or compromising the integrity and trust of a device are huge. The challenge for OEMs is how to protect a system from such attacks—early in the manufacturing stage and throughout the product life—so that device operations can be trusted in the cloud. A new paradigm shift is required to mitigate these fast-growing and looming threats.

Micron's Authenta™ Key Management Service

Enter Authenta Key Management Service (KMS). The Authenta KMS is a cloud service built to work in conjunction with Authenta-enabled flash memory deployed in standard flash memory sockets and in a wide range of Internet of Things (IoT) end-points. By leveraging silicon-based roots, Authenta KMS cloud service can widely establish early and strong protection of devices in the manufacturing stage, transferring their control to trusted parties for configuring and loading critical firmware and data.

Authenta KMS silicon-based security-as-a service

Cloud database of flash credentials and ownership keys

- Cryptographic identities provisioned in Micron fab to establish provenance, trust

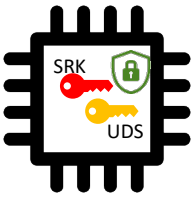
Provenance and control transfer service

- Secure hand over of flash control from Micron to trusted party for secure configuring and programming of flash memory

Delivery of strong device identities

- Cloud use cases such as secure on-boarding, secure communications, device management
- Late binding of identities and credentials to manage and protect deployed services.

The Authenta Key Management Service greatly simplifies the manufacturing flow by not requiring credentials to be exposed on the floor for service. Cryptographically signed commands are delivered to IoT end-points with Authenta-enabled flash. This trust—derived from inception—can then be pushed forward to a secure field deployment and trusted operations in the cloud.



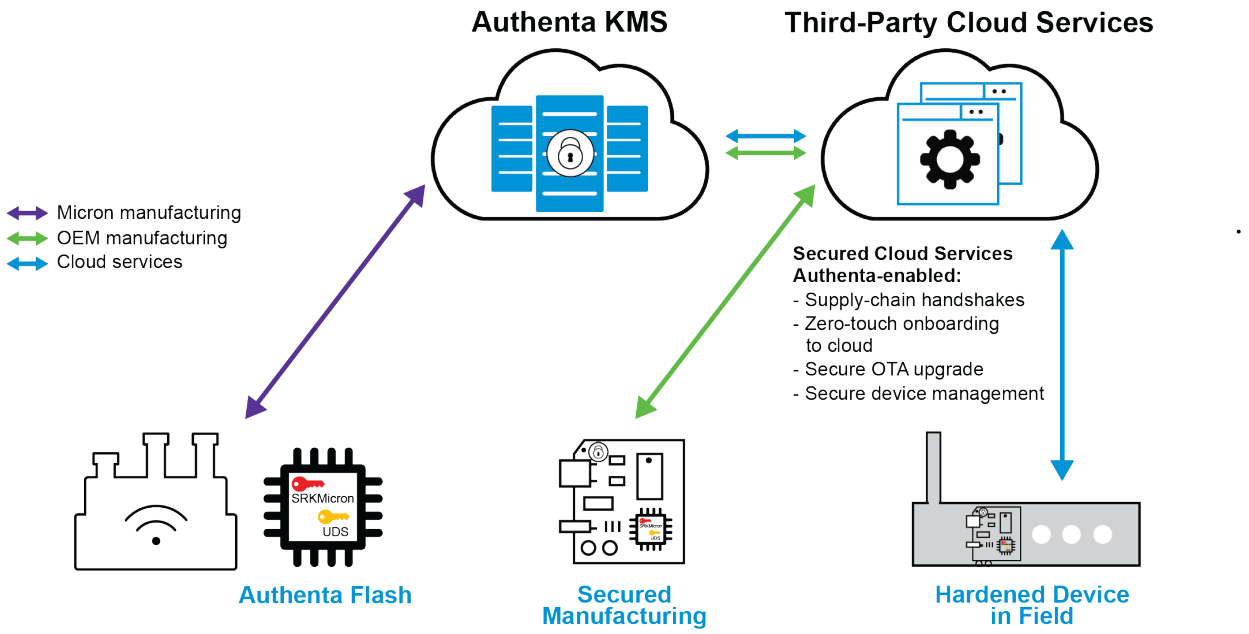
Authenta Flash

Authenta KMS

Authenta Key Management Service leverages Authenta-enabled flash to deploy strong silicon-based security-as-a service platform.

Micron

Authenta™ Key Management Service



Authenta KMS Features

Silicon-based security activation, control and protection

- Leverages integrated secure element function in flash as foundation for all security services
- Supports signed commands SHA, ECC for configuring and programming security features

Trusted supply chain handshakes

- Establishes provenance and authenticity of flash devices
- Secures delivery of device credentials used with signing commands and changing ownership
- Issuance of Change_Owner commands to disable Micron credentials for control
- **No secrets exposed on manufacturing floor**

Strong device identities for cloud services

- Secures delivery of server root keys and unique device secrets to administer device identities
- Enables zero-touch onboarding, firmware updates, device management and more
- Enables flexible delivery of identities for late binding of credentials, apps, or data

KMS database

- Micron-hosted service: HTTP, CoAp, MQTT support
- Customer registration, whitelisting for access control
- TLS communication with RSA/ECC support
- UID (User ID) index to search device credentials