MICRON AUTHENTA TECHNOLOGY: SILICON ROOT OF TRUST TO SECURE THE INTELLIGENT EDGE

FLASH MEMORY WITH EMBEDDED ROOT OF TRUST

As more IoT solutions take hold of the digital landscape, the need for security is paramount to their integrity and potential. Micron has created Authenta-enabled flash memory and a complementary edge-to-cloud cybersecurity platform to solve these security problems for IoT. This paper breaks down the challenges of IoT security and addresses how Micron's Authenta creates trusted systems and helps to secure the IoT.

THE CHALLENGE OF IOT SECURITY

With the expansion of 5G, there has been an explosion of IoT connectivity. This explosion has led to the maturation of IoT and more enterprise IoT deployments in digitally transformed businesses.

However, security concerns remain a barrier to accelerated IoT growth, while the diverse and fragmented nature of IoT leaves it even more vulnerable to attacks. Although the IoT is expected to grow even more within the next half-decade, current security practices are difficult to scale and tack on extra costs to the bill of materials.

One challenge for ODMs and OEMs is that a growing number of cyberattacks are on the manufacturing side. Security for IoT solutions should address cyberattacks at the earliest stages during manufacturing – not as an afterthought.

Should a malicious attack compromise IoT devices during manufacturing, these devices with deeply rooted vulnerabilities can be exploited further down in the supply chain or later in the device's lifecycle. Imagine, for example, the implications of a connected heart-rate monitoring device compromised with vulnerabilities during manufacturing – potentially leaving it vulnerable to cyberattacks when being used for critical patient monitoring in the hospital.

In short, the lack of security could compromise system behavior, or the critical service being provided. With IoT cloud services, this could mean dangerous portals being created into other cloud platforms. The goal of security for IoT is to create a trusted

system of connected IoT devices that can be securely onboarded, updated, monitored, and managed for the entire lifecycle – from deployment to obsolescence. There needs to be a standardized process for establishing this trust and, ultimately, a secure device identity rooted in trust by the system.

Micron Authenta Flash Memory and Authenta Cloud Platform

Micron's solution is Authenta-enabled flash memory embedded within IoT solutions and the recently launched Authenta Cloud Platform.

Authenta-enabled flash memory uniquely integrates true hardware-based silicon roots of trust (RoT) into the flash memory of a system. RoT is a concept within a system that allows for code to be authenticated within the boot processes and run within that system – thereby securing devices at their lowest layers. With the trust features embedded directly in the flash memory, Authenta assures security at the earliest stages of the device lifecycle – during manufacturing.

The value of a root of trust is that it can then be used to create an identity at the birth the device and verify trust along the supply chain. This is similar to how say, a school might grant student IDs, with identifies verified by a student's driver's license, which in turn was verified with a birth certificate – each step is authenticated along the way and traceable to an original source, meaning we can trace back any anomalies to the origin.

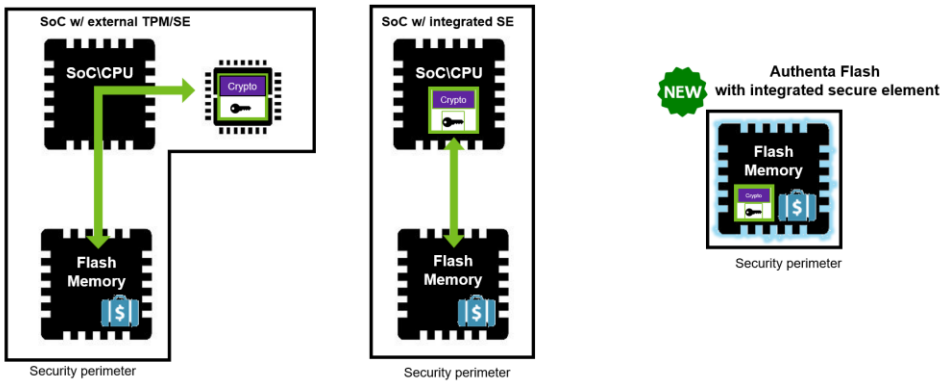
Practically speaking in terms of security, this means any hardware vulnerabilities can easily be identified and remedied. Subsequent participants in the supply chain can re-verify the credentials of the device at any stage using Authenta's RoT, building an ongoing, measurable and verifiable chain of trust.

Micron claims Authenta is one of the first technologies that takes RoT and puts it directly in the flash memory, which circumvents the challenges of placing a RoT within the SoC. This eliminates the cost of adding secure element chips or the need for key provisioning in the manufacturing flow, enabling hardware-level security at scale.

Complementing this silicon RoT technology, the Authenta Cloud Platform is Micron's new Security-as-a-Service platform which delivers the keys for the Authenta-enabled flash memory. Authenta's hardware-based RoT makes silicon-level cyberattacks harder to execute and less scalable than system, software, or supply chain attacks. RoT is established early in its lifecycle through the Authenta Cloud Platform to be passed down

to parties with Authenta flash systems, establishing the chain of trust between the device and its designated services.

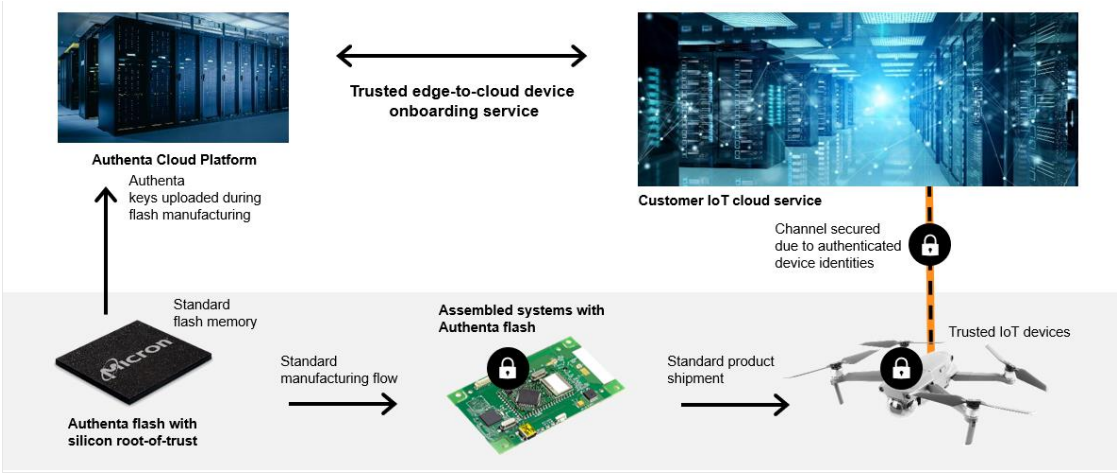
FIGURE 1: FLASH MEMORY WITH EXTERNAL TPM/SE, INTEGRATED SE AND ROT



Source: Micron

Authenta Cloud Platform makes it easy for cloud services to validate IoT devices to activate their respective services. Devices can be authenticated within the cloud, at the edge, or on the device, making it scalable for varying system setups. Because Authenta simplifies the manufacturing flow by not requiring credentials on the floor, OEMs and ODMs can focus on other issues rather than cumbersome logistics.

FIGURE 2: AUTHENTA'S ROOT OF TRUST ENABLING TRUSTED IOT SERVICES VIA CLOUD



Source: Micron

AUTHENTA IN THE MARKET

Authenta has also seen recent momentum with SanCloud, which designs IoT devices and solutions for smart buildings, smart manufacturing, and asset tracking. Applications such as connected lighting, automotive gateways, and preventative machine maintenance deliver secure and trusted data to SanTrack for analysis.

SanCloud's SanTrack IoT cloud solution uses the Authenta Cloud Platform to ensure the trust and security of these embedded devices from the manufacturing stage to secure onboarding to deployment.

In addition, Micron and Swissbit, a leading European security and memory solution provider for IoT applications, are collaborating to embed Authenta in Swissbit's security and storage solutions for IoT and industrial markets. The first Swissbit storage product with integrated Authenta technology will be a microSD card, ideal for retrofitting IoT systems; an embedded product, eMMC, will follow later.

The integration of Authenta's secure element features in Swissbit's flash storage modules gives Swissbit customers the ability to use the Authenta Cloud Platform for its simplified silicon-to-cloud onboarding and authentication capabilities. Swissbit's customers span segments such as industrial automation, automotive, IoT, medical, and networking – all areas where strong cybersecurity is crucial.

CONCLUSION

While RoT is not a new concept, placing it in flash memory and deploying it into IoT by the masses fixes many security concerns. Secure memory is crucial to disseminating trust throughout the IoT ecosystem and intelligent edge. Not only that, because memory is a ubiquitous component that gives billions of connected devices their identity, Authenta has the potential to become a key enabler of trust across the edge ecosystem.

Authenta has increasing momentum, well positioning itself as the industry standard within the IoT ecosystem. Its hardware-based zero-trust and zero-touch standards are excellent methods for the IoT supply chain and can help close critical IoT security gaps.

Micron's Authenta security for IoT offers an open and scalable foundation to power secure end-to-end cloud services across the IoT ecosystem and in doing so, can help unlock new business opportunity and innovation at the edge.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Patrick Moorhead, CEO, Founder & Chief Analyst at Moor Insights & Strategy
Jacob Freyman, Analyst at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, CEO, Founder, & Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name and title, and "Moor Insights & Strategy." Non-press and non-analysts must receive prior written permission from Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES

Micron Technologies commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.