SILICON LABS

Matter Security:
Applying Privacy Fundamentals to Smart Home Devices

Introduction

As IoT devices proliferate, companies across the industry are working to improve the development and implementation of smart home devices.

However, as innovation continues, cybersecurity risks increase. Security and data privacy are primary concerns for consumers, even to the point of limiting technology adoption. This paper introduces Matter as an IoT connectivity standard that's been designed around security and privacy, and highlights key features that ensure device security from the factory to the living room.

Formerly known as Project Connected Home Over IP (CHIP), Matter is a global connectivity standard designed to enable seamless communication across IoT devices. Through efforts by Google, Apple, Amazon, and others—including Silicon Labs—Matter makes it easier to build devices that are compatible with smart home and voice services like Amazon's Alexa, Apple Smart Home, Google Assistant, and beyond. Today, designing devices that fit into these popular ecosystems is a complex undertaking, sometimes resulting in a poor user experience. At its core, Matter is designed with device manufacturers and users in mind. With interoperable wireless standards for consumer smart home devices, the industry can move the market towards fully integrated systems.

Internet Protocol (IP) is a key element that makes Matter work for everyone. Communication across standards is made possible by IP-based networking technologies for Wi-Fi, Ethernet, and Thread. Manufacturers favor battery-powered, long-range, and low-power IoT solutions to achieve seamless connectivity for smart home technologies, and protocols like Wi-Fi and Thread - which use IP based networking - make it easy for customers to develop low power wireless IoT Matter solutions.

Matter Takes the Best Elements of Existing Technologies

Existing wireless protocols offer different benefits and one of the defining characteristics of Matter is that it's taking advantage of some of the best features provided by these technologies and brings them together.

Matter Over Thread

Thread is built on the familiar and proven IEEE 802.15.4 radio technology and offers low power and mesh networking technology for IoT products. It is IP based enabling secure cloud access. Matter runs on top of Thread and uses Threads underlying features and security capability and builds on top of that layer with added security for Matter enabled devices.

Matter Over Wi-Fi

Wi-Fi is built on the familiar and proven IEEE 802.11 radio technology and offers pervasive connectivity using widely available Wi-Fi infrastructure and IP networking. It provides easy and secure connectivity via built-in security features like WPA2/WPA3. Matter runs on top of Wi-Fi and uses its underlying features and security capabilities to further secure Matter enabled devices with its own security layer.

Matter Security and Certification

Right now, every smart home ecosystem has its own security and certification requirements. This creates confusion for developers and ultimately results in risky deployment for consumers. More protocols mean there is a larger attack surface for cybercriminals to strike.

Common attack vectors include:

- Malfunctioning via remote control or physical tampering
- Tricking devices into fallback modes, where operation is less secure
- Distributing counterfeit devices
- Denying service via Distributed Denial of Service (DDoS) attacks
- Exploiting lack of proof of possession (i.e., unprotected commissioning)

Consumers need to know they can trust their devices. Best practices for security on mobile, PC, and cloud services—including device authenticity, secure communication, and access control— are already expected by developers and consumers, and those mechanisms also protect IoT devices. However, smart home technologies present their own unique set of safety concerns when it comes to manufacturing, operations, and maintenance that Matter seeks to address.

Development and Manufacturing

The Matter Software Development Kit (SKD) was built by a large team of security-focused developers from across the industry, including Silicon Labs. It is fully open source, and the team continues working to establish a regular auditing and inspection protocol to monitor development changes.

To avoid attacks like malicious code injection while a device is in a factory in the supply chain, Matter focuses on the provisioning of device identity and firmware security. It is critical that the integrity of the device certification process is maintained based on new and emerging standards. Wireless technology designers such as Silicon Labs provide tools and devices to help developers better integrate security features into a design from the start. For example, Silicon Labs' EFR32 devices allow developers to encrypt and authenticate boot images, so any device that receives one can authenticate it.

The Connectivity Standards Alliance (CSA), which oversees Matter, also established a Security Group and a Product Security Incident Response Team (PSIRT) to process, review, and address externally reported security vulnerabilities if they arise.

Silicon Labs integrates cryptography in all EFR32 chip offerings to generate the private keys in each chip's secure element—Secure Vault™

Operation

Once set up in homes, devices are still susceptible to remote and physical attacks. To avoid and defend against these attacks, the Matter certification process ensures that every device joining a network is certified and that all messages are encrypted and authenticated once installed.

Secure connections can be unicast to one device or broadcast to many in the ecosystem to ensure that data arrives at its intended destination in a confidential and unaltered state. This strategy is accomplished with a layered approach to authentication and attestation.

Matter security is self-contained, so it does not rely on the security of any underlying communication technologies. Security measures adopted by technologies like Wi-Fi or Thread are an added level of protection, but Matter comes with reference implementations that include functional security elements in a self-contained package.

Maintenance

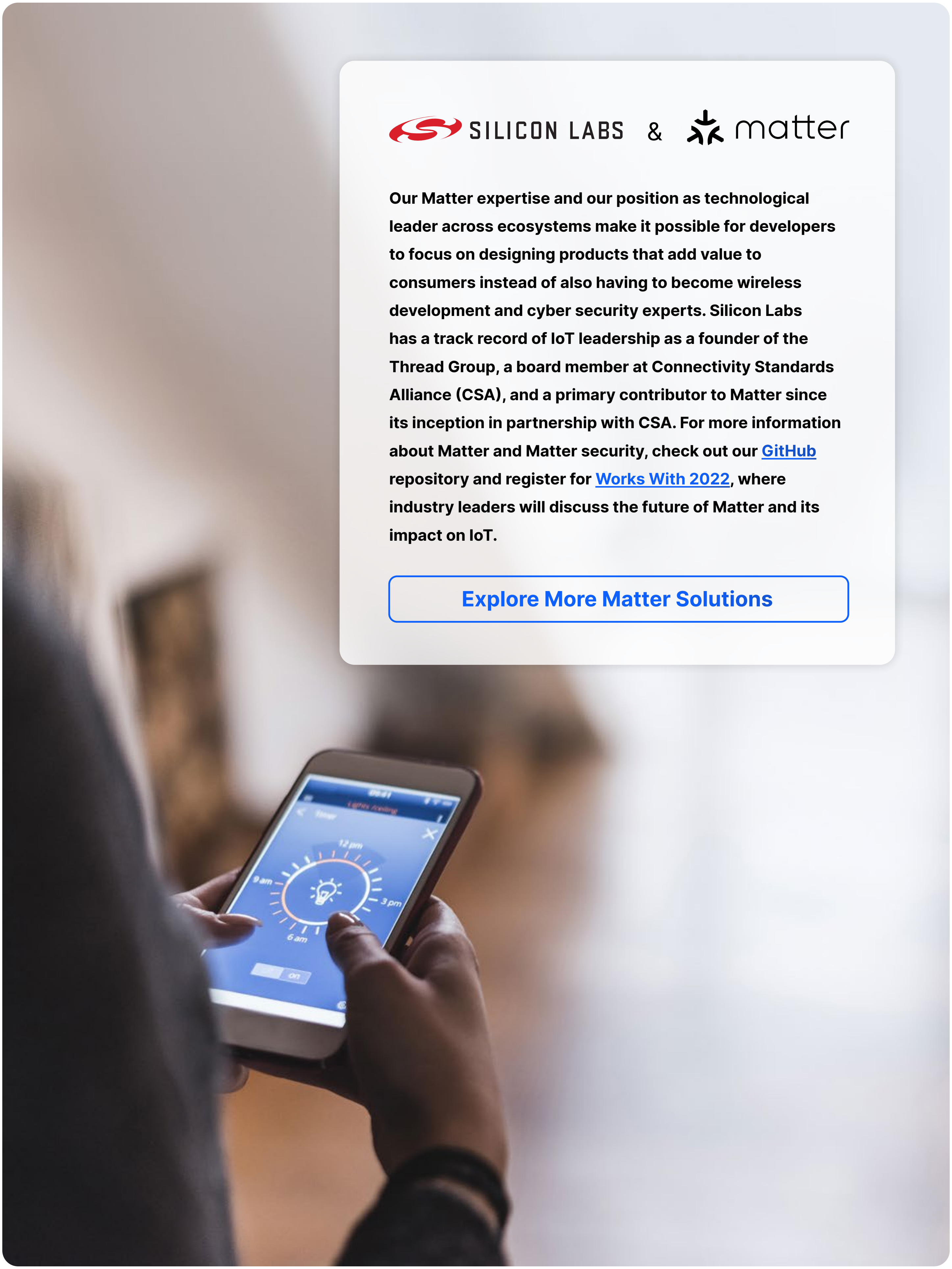
Maintaining security without maintenance mechanisms is an unrealistic expectation; a reliable update process prevents malware and unauthorized firmware from being loaded onto devices in operation.

With Matter, commissioning adheres to the most up-to-date security standards:

- Devices only gain access to Wi-Fi or Thread networks after they are authenticated
- The owner of the device provides an out-of-band device passcode to prove control
- A device cannot join a Matter network without proving its authenticity (i.e., device attestation)
- Over-the-air (OTA) firmware updates are authenticated and encrypted

A compliance ledger facilitates authentication, so a network can tell whether a device has been certified before it is allowed on the network. The ledger lists all known manufacturers and their compliant software, so if a software update is not certified, it is not allowed on the network. Each Matter device contains a manufacturer certificate and a private key to attest that the device is authentic. Silicon Labs integrates cryptography in all EFR32 chip offerings to generate the private keys in each chip's secure element—Secure Vault™, which renders the private keys untouchable, so they cannot be hacked or stolen

Maintenance also applies to the Matter protocol itself, not just devices. The core specification is designed to accommodate future versions that would adopt new cryptographic primitives without changing the whole specification unless threat analysis shows it is necessary.



SILICON LABS & matter

Our Matter expertise and our position as technological leader across ecosystems make it possible for developers to focus on designing products that add value to consumers instead of also having to become wireless development and cyber security experts. Silicon Labs has a track record of IoT leadership as a founder of the Thread Group, a board member at Connectivity Standards Alliance (CSA), and a primary contributor to Matter since its inception in partnership with CSA. For more information about Matter and Matter security, check out our GitHub repository and register for Works With 2022, where industry leaders will discuss the future of Matter and its impact on IoT.

Explore More Matter Solutions