Keyfactor for Smart Home

Making Matter-compliant devices with security by design

Establishing trust and compliance in Smart Home and consumer IoT devices with identity-first security.

Over the past decade, there has been a monumental shift in technology in the home. Previously, every device acted independently of every other device, even from the same manufacturer, with no way of communicating between the two. Now, consumers expect every device they purchase to work with every other device they own, out of the box, no matter who made it. And it needs to be easy and secure.

Security and interoperability are no longer optional for Smart Home devices

Enter Matter, a new standard for smart home connectivity. Now, manufacturers can develop against a single, unifying standard to communicate with devices from other manufacturers instead of developing against every other API on the market. This can cut time to market, cost to develop, and opens the market to newer, less established companies by making it easy to work with established competitors.

However, with a new standard comes new processes, tools, and requirements like device identities and PKI. If a manufacturer does not have experience with these technologies, it can disrupt current development and manufacturing processes leading to delays, and in turn, lost profits.

Keyfactor solutions:

Trusted PKI

The foundation for trust in connected home devices is ensuring that every component is authenticated with a unique and verifiable identity — issued from a trusted PKI.

Secure code signing

Updates are inevitable. Signing and verifying firmware and over-the-air (OTA) updates ensures that only authorized code from legitimate sources can run on smart devices.

3 unique challenges for smart home security

01 Matter compliance

Matter is rapidly becoming the de facto standard for smart home devices, and therefore, a must for manufacturers who want to gain market share. Compliance means implementing changes for software and optionally hardware to securely receive and host device attestation certificates (DAC) as well as infrastructure to generate and issue the DACs.

02 Scalability

Issuing a unique identity to every device comes with challenges, even when there's only one product line and a predictable number of units to be produced. But the goal of every business is to scale, so every tool and process must be ready to scale alongside the business.

03 Securing updates

Software and firmware updates are inevitable. To stay relevant in the market, bugs must be fixed, and new features and integrations have to be added to existing products. Additionally, Matter will continue to evolve with requirements like secure boot; this must all be done securely without adding hassle to developers.

> “Matter allows us to build new smart home integrations easier and faster, and it allows users to experience lower latency and better security."
>
> George Yianni, Head of Technology, Philips Hue at Signify
>
> https://csa-iot.org/wp-content/uploads/2022/11/Member-Company-Quote-Sheet_Nov-3.pdf

Building Matter-compliant devices with identity-first security

Security within the Matter standard has two pillars: (1) every device requires a unique, verifiable identity, and (2) code updates must be secure. Like any other network, a Matter fabric is only as secure as its most vulnerable component. Code signing and PKI-based identities are proven methods and now required for devices to be Matter compliant.

Identity issuance

To be Matter compliant, every device must have an identity and every product line must have its own product attestation intermediate (PAI). Manufacturers need to be able to do this with minimal impact to their current operations and their bottom line. While a shared product attestation authority (PAA) may have an initial appeal to stand up quickly, manufacturers should seek to maintain control and ownership with their PAA and PAIs.

Scaling with growth

As a business scales and new products are introduced, they must have a solution that can quickly and easily ramp up identity issuance. This means having the ability to rapidly expand the number of certificates being issued as well as bringing on new PAIs without requiring additional costly infrastructure or architectural changes.

Protecting code integrity

Manufacturers must ensure that only authorized code can run on devices. If transmitted through insecure channels, the code could be intercepted, altered, then pushed down to their smart devices. Unauthorized code can lead to a breach or malicious attack to gain remote control, access data, or push ransomware not just to the device, but any other device on the network.

The Solution:

PKI and code signing

With identity-first security from Keyfactor, manufacturers can protect every device with a unique and trusted identity, enable secure over-the-air (OTA) updates, and ultimately, ensure that devices are safe, secure, and Matter-compliant from design to end-of-life. Trusted by some of the largest IoT manufacturers, Keyfactor delivers identity issuance, governance, and operational efficiency at the scale the IoT market demands.

Scalable and flexible PKI

Using EJBCA Enterprise, a highly scalable and flexible PKI platform, product design and security teams can issue trusted certificate-based identities to connected devices at a massive scale, whether during manufacturing or in the field. EJBCA PKI can be deployed within the data center, in the cloud, as a managed service, or even on the manufacturing floor.

Keyfactor EJBCA Enterprise

Learn more ↗

Secure code signing

SignServer Enterprise digitally signs firmware and validates signatures to ensure only trusted code is executed on connected devices and systems. The solution can leverage your existing on-premises or cloud-based hardware security module (HSM) or use a built-in HSM with a turnkey hardware appliance.

Keyfactor SignServer Enterprise

Learn more ↗

Certificate lifecycle automation

Leveraging Command for IoT, manufacturers get complete visibility and lifecycle management of all keys and certificates issued in their infrastructure and on their devices, allowing teams to revoke, renew, and re-issue millions of certificates in bulk from a single platform to ensure identities remain secure over the device's lifespan.

Keyfactor Command for IoT

Learn more ↗

Key benefits of identity-first security from Keyfactor

- ✓ Build Matter-compliant devices with a trusted partner
- ✓ Retain full control and ownership of your PKI solution
- ✓ Scale easily with a growing demand and product portfolio
- ✓ Ensure software and firmware are securely updated throughout the device's lifecycle
- ✓ Implement a PKI with flexible architecture to meet the needs of both today and tomorrow
- ✓ Prepare for the evolution and upcoming requirements of future releases of Matter

Want more information about Keyfactor for smart home cybersecurity?

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1.216.785.2946