NXP EdgeLock® SE051

Use Case:
Smart Home Security – Matter

For smart homes to be truly smart, the devices that connect to the home network and the cloud need to be both interoperable and secure. The new Matter standard, enabled by NXP solutions, delivers the seamless, secure connectivity that lets smart homes live up to their promise.

APPLICATIONS

Smart Home Control

Smart Home Entertainment

Smart Home Security

Smart Home Gateway

CHALLENGE

People around the world are installing systems that make their homes smarter, more connected, more convenient, more energy efficient, more entertaining, and more secure. But device diversity and lack of interoperability can cause frustration during setup and make it difficult to establish, maintain, and expand a smart-home network.

What's more, connected devices in the smart-home environment can become an entry point for hackers. There are a number of ways for hackers to gain access to smart-home devices and, once they do, access to the full home

network and just about every aspect of private life – personal information, financial data, security systems, home safety – is at risk.

From the device manufacturer's standpoint, market fragmentation makes it difficult to develop a comprehensive approach to security. There are many different individual

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

actions and vulnerabilities to protect, yet the high degree of protocol and ecosystem diversity makes it difficult to approach security as a whole. For each ecosystem manufacturers design for, they have to learn and support a different set of security mechanisms.

Particular areas of concern include when devices are first onboarded onto the network, when devices communicate within the home network and how these devices can protect against new threats once deployed. At all points, the device and its connection needs to be secured by a unique device identity. Developing a secure process for creating and assigning device identities is a complex task, involving extreme vigilance and multiple layers of protection in the production phase. Device manufacturers have to consider how the provisioned identity is stored on the device and how to manage device credentials to minimize its vulnerability. The methods for provisioning and credential management vary with each ecosystem, adding yet another layer of complexity to the development and delivery of smart devices.

SOLUTION

An industry-wide effort, driven by the Connectivity Standards Alliance (CSA) and NXP, offers the interoperability and security that smart-home devices need. The CSA's new standard, called Matter*, is a single, unified application-layer connectivity protocol designed to enable developers to connect and build reliable, secure IoT ecosystems and increase compatibility among smart home and building devices.

By increasing interoperability and security across smart-home ecosystems, the Matter standard promises to simplify development for product manufacturers while making installation simpler and more secure and ensuring high-level security at every point for consumers. With Matter's layered and strong approach to security, smart-home devices can offer authenticated onboarding, along with secure connection to the home network. Data can be encrypted and then transmitted over the network, to prevent data sniffing, and locally stored data can be protected using encryption keys. For both secure onboarding and secure communication within a Matter home network, standardized cryptographic protocols are included in the Matter specification. These protocols ensure compatibility between all Matter devices and are chosen on the basis of their security level. Matter

---

* Matter was originally introduced as Project CHIP by the Zigbee Alliance, which is now the Connectivity Standards Alliance.

also defines an update mechanism providing deployed devices the ability to address new developments in security and threats.

The Matter standard makes security an integral part of operation and requires the use of certain crypto protocols. The EdgeLock SE051, a tamper-resistant secure element that ensures the confidentiality, integrity, and authenticity of device communications, is a turnkey solution for supporting Matter cryptography and security protocols implemented and accelerated in hardware, such as ECDSA and AES-CCM.

The EdgeLock SE051 provides higher-level, certified security for Matter-based devices, so developers can simplify development while differentiating their products. The EdgeLock SE051 comes with certified hardware and cryptographic algorithms, and a middleware stack that simplifies integration and strengthens the security of any embedded architecture, including those that use a secure MCU/MPU equipped with high-level protections. The EdgeLock SE051 is independently certified at CC EAL 6+.

The EdgeLock SE051 is also supported by NXP's EdgeLock 2GO service for provisioning devices with the identities and credentials required for onboarding the devices into the Matter ecosystem. With EdgeLock 2GO, NXP offers a tailored provisioning service so that device manufacturers don't have to invest in new manufacturing equipment for supporting the security requirements of Matter. The result is quick deployment of "connect and go" smart-home devices that are easy to commission.

As an extended hardware crypto offering, complete with SEMS technology and supported by NXP updates, the EdgeLock SE051 is designed to stay current with Matter specifications as they evolve.

LEARN MORE

The NXP Design Community site offers helpful hints, easy-to-follow how tos, and detailed application notes for use with the EdgeLock SE051. The EdgeLock SE051 Product Page links to detailed specs, designs tools & software, training & support, and more.

▸ **NXP Design Community**
   community.nxp.com/community/identification-security/secure-authentication/overview

▸ **EdgeLock SE051 Product Page**
   www.nxp.com/SE051