NXP EdgeLock™ SE050

Use Case:
Secure Cloud Onboarding

Adding a secure element to an IoT device makes it possible to deploy secure, zero-touch connections to public and private cloud services, edge computing platforms and infrastructures, for end-to-end security from chip to cloud.

APPLICATIONS

Smart City

Industrial

Smart Home

CHALLENGE

The widespread availability of subscription-based cloud connectivity makes the IoT more accessible to everyday products and expands the range of IoT-driven services. With this increased use of the cloud, however, comes increased vulnerability.

IoT devices are often the targets of cyberattacks. Devices with inadequate protections can reveal private user information and can supply hackers with the data needed to create their own counterfeit devices. Compromised IoT devices can also be used to mount attacks on the network, making it possible to access other connected devices and backend enterprise resources.

Unauthorized access to just one device can have a domino effect, causing widespread network damage and even threatening public safety, since so many IoT devices are

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

used in applications, such as building automation, transport, utilities, and healthcare, with a direct impact on people and their communities.

To protect cloud connections and ensure safe operation, the keys and certificates used by an IoT device to authenticate a cloud connection need to remain securely stored, and any data sent by the device needs to remain encrypted and secured while in transit.

SOLUTION

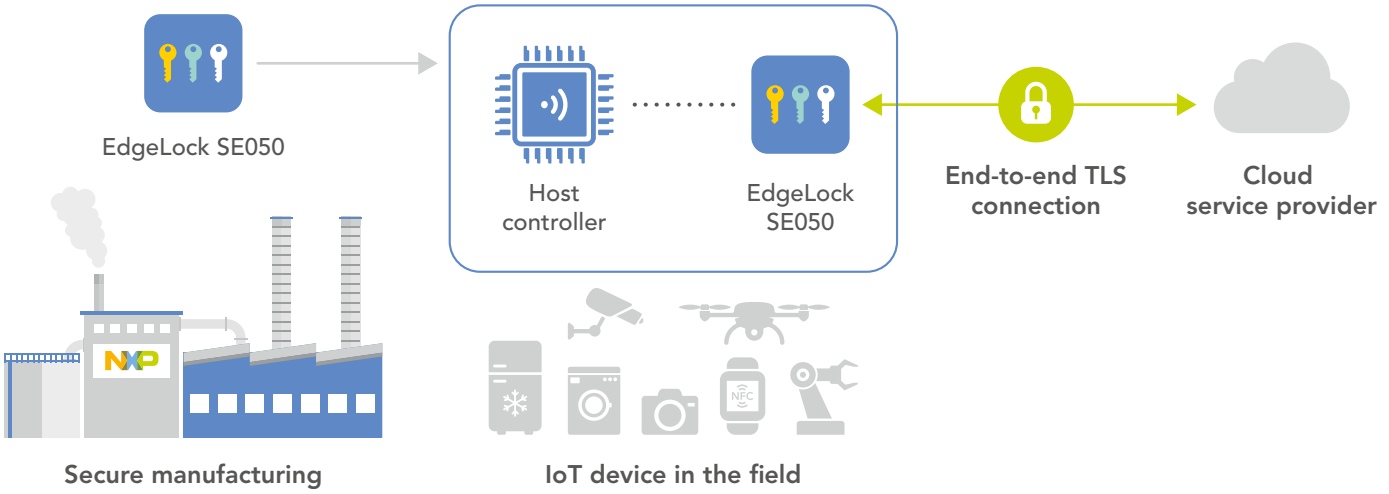
The EdgeLock SE050 is a tamper-resistant platform that protects the keys and certificates used for device authentication. The EdgeLock SE050 also establishes a trusted TLS channel for secure connectivity with different cloud service providers.

The EdgeLock SE050 applet supports TLS version 1.3 and pre-shared key cipher suites using either symmetric keys or ephemeral keys, which is the format preferred by today's major public IoT cloud providers.

What's more, the EdgeLock SE050 comes with pre-provisioned security credentials, which can be used for cloud onboarding. Because the credentials never leave the IC, the chain of trust is preserved during the entire product lifecycle. The result is true end-to-end security for IoT devices.

The SE050 connects to the host processor using an I^2C slave interface. Connection to the cloud is established by Plug & Trust middleware, which uses the pre-provisioned credentials in the SE050 as part of the TLS handshake. Once the cloud connection has been established, the session key is exported to the host processor, thereby removing the SE050 from the rest of the encryption/decryption handshake.

BLOCK DIAGRAM



LEARN MORE

The NXP Design Community site offers helpful hints, easy-to-follow how to's, and detailed application notes for use with the EdgeLock SE050. The EdgeLock SE050 Product Page links to detailed specs, designs tools & software, training & support, and more.

- **NXP Design Community**
  https://community.nxp.com/community/identification-security/secure-authentication/people
- **EdgeLock SE050 Product Page**
  www.nxp.com/SE050

Find more information on **www.nxp.com/SE050**

Date of release: December 2019