NXP
EdgeLock® SE050

Use Case: *Secure, FIPS- and Matter-Compliant IP Cameras*

As prime targets for cyberattacks, IP cameras are some of the most vulnerable devices in the Internet of Things (IoT). NXP offers a turnkey security solution for IP cameras that turns what would otherwise be serious security risks into trusted assets for video monitoring.

APPLICATIONS

Smart Home

Smart City

Industrial

CHALLENGE

IP cameras present a number of risks. They're often used in sensitive applications, such as security and surveillance, which attract hackers. Manufacturing and other industrial applications also use IP cameras as part of essential business processes, which means business-critical tasks, such as late-stage configuration, in-field updates, smart analytics, and periodic maintenance, can be hijacked or abused. What's more, installation in unsupervised locations creates opportunities for physical attacks and, because IP cameras have a relatively high degree of functionality, they're attractive targets for use in network strikes, such as Distributed Denial of Service (DDoS) attacks.

At nearly every point in the IP camera's life cycle there are opportunities for manipulation or theft. If the IP camera is manufactured at an untrusted facility, security credentials can be tampered with prior to shipment.

PLUG &TRUST

Securing tomorrow's IoT. *Today.*

During installation, hackers can steal the private information used for legitimate access. Every session with the cloud presents an opportunity to spoof the authentication process, and any video transmission can be stolen or modified as part of a deepfake attack. The rise of fake images, created by artificial intelligence (AI), makes is all the more important to be able to verify the origin and validity of footage.

Given so many points of risk with IP cameras, security needs to be a fundamental part of device operation. Fortunately, there are a number of security certifications that can guide development and help ensure devices use industry-recognized protections. In the North American market, for example, devices that are FIPS 140-2 certified are verified to use proven encryption algorithms, and devices that conform to the Matter specification, for Smart Home, have built-in security mechanisms.

To pass certification, IP cameras need to store and protect sensitive information, such as credentials and security keys. A growing number of standards, including Matter, require devices to use silicon, and not software, for storage and protection. Adding a silicon-based root of trust, in the form of a secure element, protects vulnerable transactions of all kinds, and helps ease certification.

SOLUTION

The NXP EdgeLock SE050 secure element is a turnkey solution that gives developers an easier path to security certification while making security an essential part of the design, relevant to every aspect of functionality.

By delivering certified security with tamper resistance, along with Common Criteria EAL 6+ certification as well as protection from the latest attack scenarios, including advanced hardware attacks, the EdgeLock SE050 delivers lifecycle protection for IP cameras.

Hardware-based security ensures safe operation, including secure key and credential storage, verified proof of origin, and safe execution of secure algorithms, and protects the essential steps in IP camera operation:

- **Secure cloud onboarding:** By delivering end-to-end security, from chip to edge to cloud, the EdgeLock SE050 makes onboarding a zero-touch event. Keys are never exposed to any party during the lifetime of the device.
- **Device-to-device authentication and attestation:** The EdgeLock SE050 supports mutual authentication, ensuring only authorized devices access the network, and uses encryption to attest the authenticity of data.
- **Late-stage parameter configuration:** EdgeLock SE05x variants integrate an ISO/IEC 1443 interface, for use with NFC, so smartphones or contactless readers can safely configure the IP camera by installing a specific setup or loading data.
- **Wi-Fi credential operation:** The EdgeLock SE050 protects the Wi-Fi credentials, including WPA2 passphrases and secret keys, used to authenticate and validate devices before allowing them to use a WLAN or Wi-Fi connection.

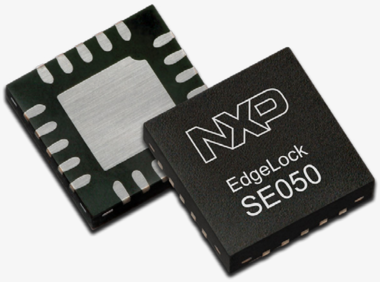
To support FIPS certification, for example, the EdgeLock SE050 is available as a module that serves as a ready-to-use certified platform with security Level 3 for the OS and app, and security Level 4 for the physical security of the hardware.

To support Matter certification, dedicated EdgeLock secure element and secure authenticator solutions provide full, turnkey Matter security. These Plug & Trust security components, which connect to any type of processor using a standard I^2C interface, are provisioned with Matter attestation keys and certificates to the device and provide hardware-accelerated execution of Matter authentication protocols for interoperability.

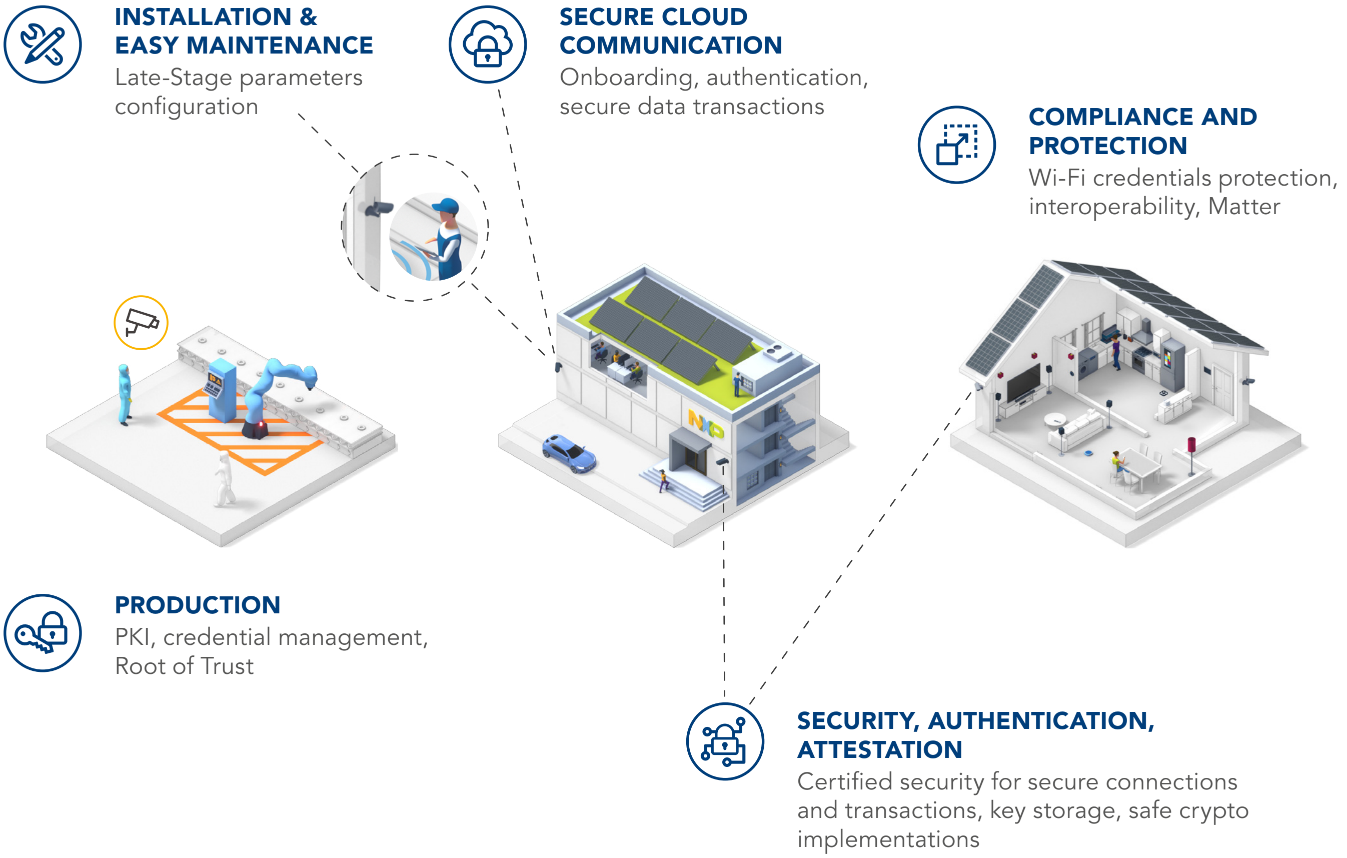
LEARN MORE

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

- NXP Design Community
- EdgeLock SE050 Secure Element Product Page



BLOCK DIAGRAM



INSTALLATION & EASY MAINTENANCE
Late-Stage parameters configuration

SECURE CLOUD COMMUNICATION
Onboarding, authentication, secure data transactions

COMPLIANCE AND PROTECTION
Wi-Fi credentials protection, interoperability, Matter

PRODUCTION
PKI, credential management, Root of Trust

SECURITY, AUTHENTICATION, ATTESTATION
Certified security for secure connections and transactions, key storage, safe crypto implementations

The EdgeLock SE050 Secure Element Offers Full Life-Cycle Protection for IP Cameras

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

Date of release: May 2023