Fact Sheet

EdgeLock® SE052F

Out-of-the-box Security for the IoT with FIPS 140-3 Level 3 Certification

As the first hardware IoT and Industrial secure element certified to FIPS 140-3 Level 3, the EdgeLock SE052F combines protection and convenience, making it easier to develop and deliver a broad range of secure, differentiated IoT devices.

Target Applications

- Industrial IoT applications that benefit from FIPS 140-3 certification
- Smart City: access, infrastructure, surveillance, etc.
- Industrial: building control, factory automation, healthcare, etc.
- Smart Infrastructure: wired and wireless network equipment and gateways
- Smart Home: home control, security systems, etc.

As the need for IoT security increases, and more government agencies require FIPS certification, manufacturers are using NIST FIPS compliance to meet regulatory requirements and indicate advanced security capabilities. The EdgeLock SE052F, a ready-to-use platform for secure IoT operations, runs cryptographic functionality and is a crypto module certified to the latest version of FIPS (140-3), and provides out-of-the-box FIPS compliance. Designed as a turnkey solution, it simplifies delivery of secure, differentiated IoT devices.

Key Features

- Certified to FIPS 140-3 Level 3 overall and to level 4 for the physical security of the hardware
- Common Criteria (CC) EAL 6+ certified
- Cryptographic functionality: ECC and RSA encryption
- Flexible design-in: I²C target, controller, and ISO/IEC 14443; 100 kB user memory, extended temp range (-40 to +105 °C), HVQFN20 package (4 x 4 mm)
- Software enablement and out-of-the-box FIPS compliance for fast-time-to-market
- EdgeLock 2GO for hassle-free device provisioning

Key Benefits

- Turnkey security solution, with comprehensive support from coding to certification
- Easy scalability, with one platform for multiple use cases and security architectures
- Straightforward certification and standard compliance, with validated FIPS and CC certification
- Fast deployment, with easy FIPS certification and NXP support for zero-touch device provisioning

With the EdgeLock SE052F, devices targeting smart city, smart factory, and other Industrial IoT use cases can provide highly secure functionality while complying with the latest FIPS requirements.

Internationally recognized as a trustworthy approach for application security, the FIPS standards, officially known as the Federal Information Processing Standards, are developed and maintained by the US National Institute of Standards and Technology (NIST). In 2021, NIST launched the new FIPS 140-3 standard, an update to the compliance requirements for products certified for use by government departments and agencies within the US and Canada.

Device manufacturers can approach FIPS compliance in one of two ways. They can certify the entire IoT device or they can use a FIPS-certified cryptographic module to run security-related operations. FIPS 140-3 provides four increasing, qualitative levels of security, intended to cover a wide range of potential applications and environments. The EdgeLock SE052F is certified as a cryptographic module to level 3 of FIPS 140-3 for the OS and applet, and to level 4, the highest available, for the physical security of the hardware.

Comprehensive Security

Not only is the EdgeLock SE052F the industry's first hardware secure element for Industrial IoT applications to be FIPS 140-3 Level 3 certified, it's also certified to Common Criteria EAL6+, the gold standard for hardware-based secure elements. Pre-validation for FIPS and CC EAL certification means developers can save time, effort, and cost when delivering new products, since there's no need to pursue their own validation efforts. The EdgeLock SE052F also features cryptographic functionalities, such as ECDSA and ECDH/E, based on NIST and Brainpool curves, as well as RSA up to 4K (including key generation), and authenticated AES encryption modes CCM/GCM.

Flexible Design-In

To help developers differentiate their products, the EdgeLock SE052F offers flexible memory management and extended memory of up to 100 kB. Also, all SE05x variants are MCU/MPU agnostic, so developers can quickly scale security across different architectures and applications.

Turnkey Solution

The EdgeLock SE052F platform includes a comprehensive product support package, including applets and middleware, so developers spend less time coding and can quickly integrate security into their projects. NXP takes care of the security and certification aspects of design, so developers can focus on the features that make their designs stand out from the competition.

Zero-Touch Device Provisioning

Device manufacturers can leverage NXP's proven EdgeLock 2GO service, which provides a secure infrastructure for key management, and can use the EdgeLock SE052F's large user memory to store credentials. There's no need to modify the in-place delivery infrastructure or find a new supply-chain partner who will inject key material.

Item	Orderable Part Number	Temperature Range	12NC
EdgeLock SE052F Ready	SE052F2HN2/ Z019HJ	-40 to +105 °C	9354 551 73118
EdgeLock SE052F Development Board	OM-SE052ARD	-40 to +105 °C	9354 567 55598

Visit nxp.com/SE052F

Document Number: ELSE052FFSA4 REV 0

FIPS 140-3™

FIPS 140-3 validated, Certificate #4679