NXP
EdgeLock® SE05x
& EdgeLock A5000

Use Case: *Qi 1.3 Wireless Charging Authentication*

Using wireless chargers that aren't Qi certified can create safety and security risks for devices and their users. NXP offers a turnkey solution for Qi 1.3 wireless charging authentication, so it's easy to deliver safe, satisfying charging experiences.

APPLICATIONS

Smartphones

Mobile and Computing Accessories

Small Appliances

Batteries

CHALLENGE

The de facto standard for cable-free charging is Qi (pronounced "chee"), a specification defined by the Wireless Power Consortium (WPC). Qi charging couldn't be simpler to use – just set the device on the charging pad – but placing a device on a charger that hasn't passed Qi certification can be dangerous, because non-approved, unauthorized Qi chargers can cause permanent damage to the receiver device or, worse yet, spark a fire or explosion.

To ensure that Qi products are safe, effective, and compatible across the Qi ecosystem, the WPC uses a strict certification program that has broad industry support. Qi certification delivers confidence – to manufacturers and consumers alike – and more than 8,250 products are registered in the WPC's database of Qi-certified products.

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

The latest version of the WPC specification, Qi v1.3, adds an extra layer of protection for charging. Qi v1.3 defines two major power profiles: the Baseline Power Profile, which delivers up to 5 watts output, and the Extended Power Profile, which delivers a maximum of 15 watts for what is called "fast charging." To safeguard devices and their users, the Extended Power Profile requires use of hardware-based authentication. Before sending any power, the wireless charger must first provide proof (authentication) that it has passed Qi v1.3 certification. The authentication step ensures that smartphones and other devices can accept the charger's 15-watt output without risking the safety of the device or the user.

To pass Qi v1.3 certification, the Extended Power Profile must use a tamper-resistant subsystem that protects the private key and certificate used for authentication. More specifically, each wireless charger unit must contain a unique private key and a unique certificate, called the Product Unit Certificate. The Product Unit Certificate must be issued by a provider who complies with the security requirements specified by the WPC, known as an Approved Manufacturer Certificate Authority (CA) Service Provider.

Designing and implementing the necessary tamper-resistant subsystem, and then establishing a secure process for issuing and injecting Product Unit Certificates, requires time and effort, and often involves specialized techniques that are unfamiliar to many hardware and software engineers.

SOLUTION

NXP has been designated an Approved Manufacturer CA Service Provider by the WPC and offers a turnkey solution for certified Qi charging with 1.3 authentication, so it's easy for manufacturers to deliver Qi-compliant devices that deliver safe, satisfying charging experiences.

We issue a Product Unit Certificate for each wireless charger. The certificate is signed by a Manufacturer Certificate Authority, created specifically for the device manufacturer and itself signed by the WPC Root Certificate Authority.

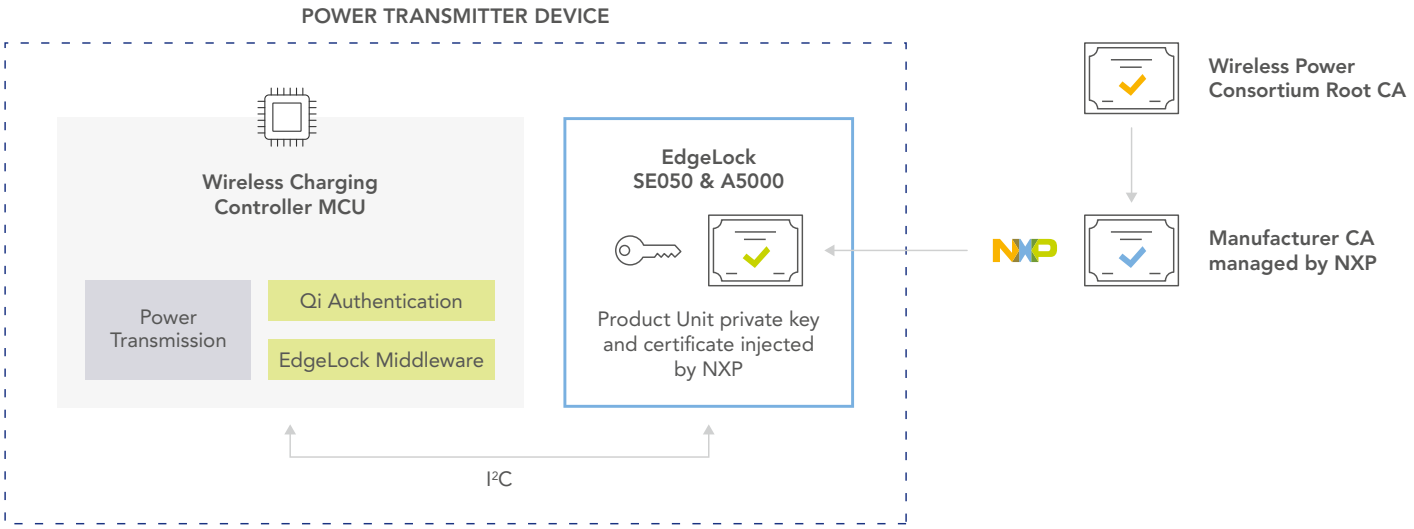
The Product Unit Certificate and its corresponding private key can be secured by the NXP EdgeLock SE05x secure element or the NXP EdgeLock A5000 secure authenticator, two WPC-compliant ICs. The EdgeLock SE05x and the EdgeLock A5000 store and protect the Qi private Product Unit key and certificate, and support ECC NIST-256 for implementing Qi Authentication messages.

The EdgeLock A5000 is tailored for basic wireless charging, while the EdgeLock SE05x supports additional use cases, for devices that, in addition to wireless charging, also support features like secure connection to the cloud or interoperability with the new IP-based Matter specification for connectivity.

The hardware configuration includes an IoT applet for ECDSA and other cryptographic operations, and is available with middleware that facilitates communication with the host. The EdgeLock SE05x and EdgeLock A5000 use the I^2C protocol, so they can be attached to just about any microcontroller or microprocessor, and are tailored for device authentication, so they deliver optimal performance while minimizing the amount of computing resources required on the host. Example source code and documentation, supplied with the EdgeLock SE05x and EdgeLock A5000, gives developers a head start on charger design and makes it easier to pass certification.

Also, as part of NXP's EdgeLock 2GO service, we can provision the EdgeLock SE05x or EdgeLock A5000 with the private Product Unit keys and certificates required for Qi authentication. There's no need to establish a costly and complex PKI infrastructure, and charger production can take place in third-party facilities without adding security risk.

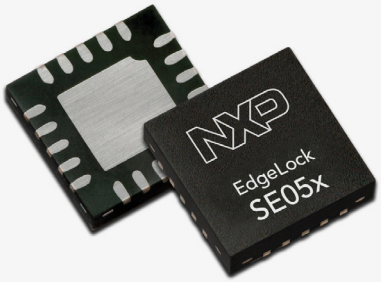
BLOCK DIAGRAM

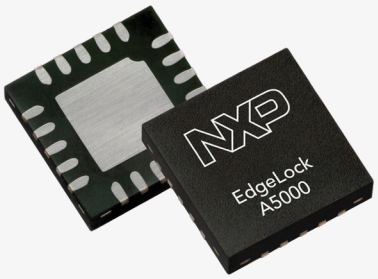


LEARN MORE

The NXP Design Community site offers helpful hints, easy-to-follow how to's, and detailed application notes for use with the EdgeLock SE050 and EdgeLock A5000, while our product pages link to detailed specs, designs tools & software, training & support, and more.

- NXP Design Community
- EdgeLock SE050 Secure Element Product Page
- EdgeLock SE051 Secure Element Product Page
- EdgeLock A5000 Secure Authenticator Product Page
- Code examples for Qi 1.3 Authentication with EdgeLock SE050 or EdgeLock A5000
  And also available as part of the EdgeLock SE05x Plug & Trust Middleware
- **Wireless Power Consortium Pages for:**
  Qi – Mobile Computing
  The Qi Authentication System





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

Date of release: June 2022