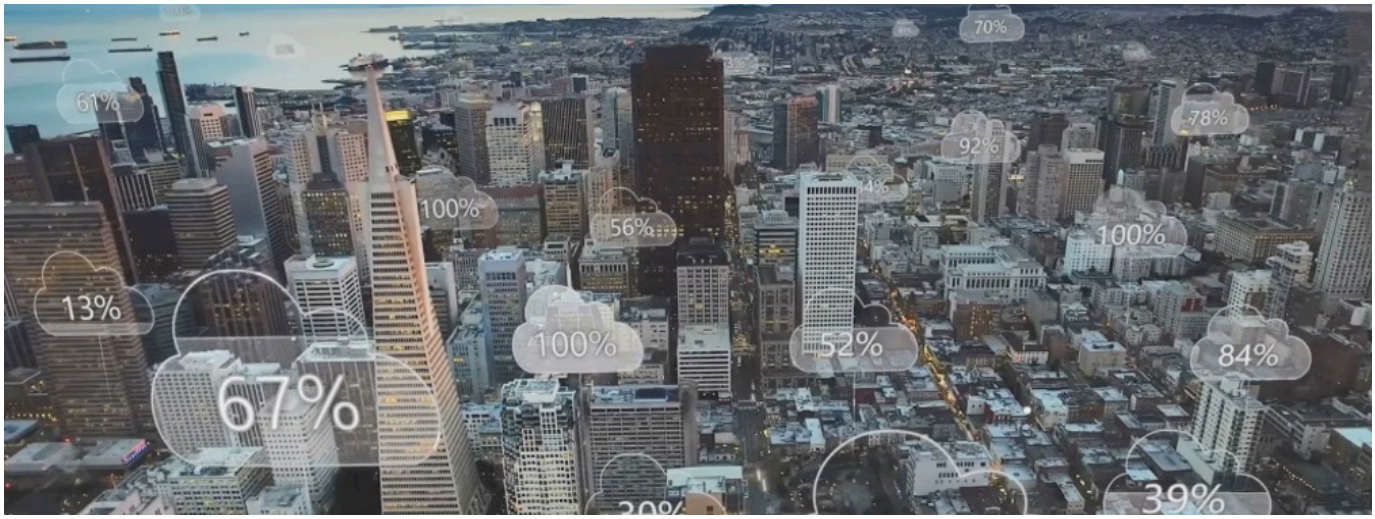
PLUG & TRUST: AUTHENTICATION MADE SECURE, SCALABLE AND EASY



The EdgeLock A5000 secure authenticator (SA) offers Common Criteria EAL 6+ certified security, with symmetric and asymmetric crypto, for simple IoT use cases, complementing NXP's EdgeLock secure element (SE) family portfolio with an authentication-optimized product.

KEY BENEFITS

- Plug & Trust for fast and easy design-in with dedicated product support package for authentication
- Ready-to-use example codes for authentication use cases
- Turnkey solution to reach system-level security with any MCU/MPU without the need to write security code or handle critical key material
- Supports compliance to many authentication security standards like DLMS/COSEM, Qi 1.3 and ISO15118-2
- Trust anchor for authentication devices with secure credential injection at hardware level

KEY FEATURES

- Certified Common Criteria (CC) EAL 6+ HW with dedicated authentication software
- PKI cryptography based on ECC NIST P-256 and P-384
- ECDSA, ECDH/ECDHE
- 3DES and AES (AES modes: CBC, CTR, ECB, CCM, GCM)
- HMAC, CMAC, GMAC, SHA-256/384
- HKDF, PRF (TLS-PSK)
- DRBG/TRNG compliant to NIST SP800-90A/B
- Secured flash user memory up to 8 kB
- I^2C target (up to fast speed mode, 1 Mbit/s)
- Secure binding with host MCU/MPU, and bus encryption
- Secure credential injection with end-to-end encryption
- Advanced access control policies to credentials and data stored on chip
- Extended temperature range (-40 to +105 °C)
- Small and very thin HXQFN20 package particularly suited for space limited applications (3 mm x 3 mm x 0.33 mm)
- EdgeLock 2GO enabled for flexible credential customization and over-the-air key management

TARGET APPLICATIONS

- Energy Management Systems and Smart Metering
- EV Chargers, Battery Systems and eBikes
- Smart Home
- Mobile Accessories
- Gaming
- Medical and Sensors
- Computing

ENSURING SECURE AUTHENTICATION

More and more devices nowadays are required to communicate only upon successful authentication, since devices can serve as an illicit point of entry to a network, a site, a system or a service. To provide the necessary levels of trust for applications where authentication is crucial, and protect against the latest attack scenarios, NXP offers the authentication-optimized EdgeLock A5000.

The pre-installed authentication software eliminates the need to write security code and the scalable, ready-to-deploy software has built-in protections that prevent unwanted modification.

AUTHENTICATION MADE SECURE, SCALABLE AND EASY

The EdgeLock A5000 is optimized for simple IoT implementations related to authentication and cloud onboarding. The product comes with secure software and credentials stored in hardware and fully isolated from external software access. There's no need to handle confidential keys nor to implement secure code at untrusted stages of the supply chain.

With this, NXP provides a scalable solution for many authentication applications where security is crucial throughout the product lifecycle.

ENABLING EASY PRODUCT DESIGN-IN

Delivered as a turnkey solution, the EdgeLock A5000 includes a dedicated product support package that simplifies the design of authentication applications and reduces time-to-market. The support package includes documentation and software libraries for the integration with the most common OSs and for different MCUs and MPUs. This allows customers to focus only on the application-specific development and accelerate the final system integration.

USE CASE ENABLEMENT

- **Device Integrity and Data Protection, Attestation and Traceability:** Allow to verify the originality of the devices and ensure that the data is signed and authenticated by the EdgeLock A5000.
- **Device-to-Device Authentication:** Ensure only authorized devices connect to a given network, site, or service with mutual authentication and hardware-protected keys.
- **Secure Credential Storage and Provisioning for Zero-Touch Cloud Onboarding:** Use zero-touch secure connectivity, based on proven, hardware-based security algorithms, to connect with public and private clouds.
- **Qi 1.3 Wireless Charging Authentication:** Integrate the EdgeLock A5000 into your wireless charger to securely store the private key and certificate of the charger and prove it is an authentic Qi-certified product.
- **Matter Ready:** Provide the necessary cryptographic functions to support the upcoming Matter standard for connecting smart home devices.

Part	Orderable Part Number	Description	Temperature Range	12NC
A5000R	A5000R2HQ1/Z016UZ	Certified SA with ECC NIST and AES for authentication use cases	-40 to +105 °C	9354 262 25472
A5000 Dev Kit	OM-A5000ARD	A5000 Arduino® compatible development kit	-40 to +105 °C	9354 243 19598

www.nxp.com/A5000

Document Number: EDGELOCKA5000FS REV 0

Certified EDGELOCK® ASSURANCE by NXP

PLUG&TRUST