

NXP Communicator

EdgeLock® A5000

Plug & Trust Secure Authenticator



NXP, the NXP logo, EdgeLock, Kinetis and MIFARE are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2022 NXP B.V.

www.nxp.com/A5000



Product Summary

OVERVIEW

Plug & Trust: Authentication made secure, scalable and easy

The EdgeLock A5000 secure authenticator (SA) offers Common Criteria EAL6+ 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.

[IoT Security Use Cases](#)

[Certified EdgeLock Assurance](#)

The EdgeLock A45000 is part of the Certified EdgeLock Assurance program, is designed to meet industry standards and follows NXP's security-by-design approach. It has been certified by an independent lab.

Ref www.nxp.com/A5000

1 EdgeLock A5000 Specification Highlights

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
- Trust anchor for authentication devices with secure credential injection at hardware level

KEY FEATURES

- Certified Common Criteria (CC) EAL6+ 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
- I²C 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)

2 Target Applications and Use Cases

TARGET APPLICATIONS

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

USE CASES

- **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.

3 Part Attributes

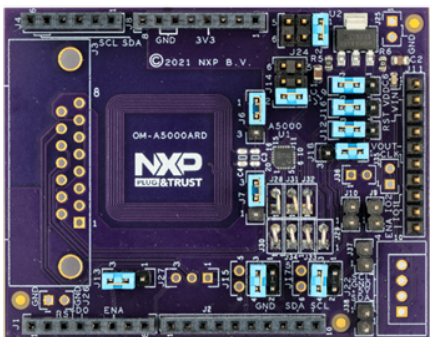
Product Description EdgeLock A5000		
EdgeLock secure authenticator with symmetric and asymmetric crypto for authentication use cases		
ECC Crypto Schemes	ECDSA	✓
	ECDH/ECDHE	✓
Supported Elliptic Curves	NIST (256, 384)	✓
Symmetric Crypto Algorithm	3DES (2K, 3K)	✓
	AES (128, 192, 256)	✓
AES Modes	CBC, ECB, CTR	✓
	CCM, GCM	✓
MAC	HMAC, CMAC	✓
	GMAC	✓
Hash Function	SHA-256, SHA-384	✓

Key Derivation (KDF)	TLS (KDF, PSK)	✓
	HKDF	✓
Secure Channel	Secure Channel Host-SE (Platform SCP)	✓
Pre-Provisioned		✓
TRNG		NIST SP800-90B, AIS31
DRBG		NIST SP800-90A, AIS20
User Memory – Maximum - NV		8 kB
Interfaces	I2C Target	✓ (up to 1 Mbit/s)
Temperature Range		-40 to +105 °C
Package		HX2QFN20

Short table part attributes:

Part	Orderable Part Number	Description	Temperature Range	12NC
A5000	A5000R2HQ1/Z016UZ	EdgeLock secure authenticator with symmetric and asymmetric crypto for authentication use cases	-40 to +105 °C	9354 262 25472

4 Development Tools and Ecosystem

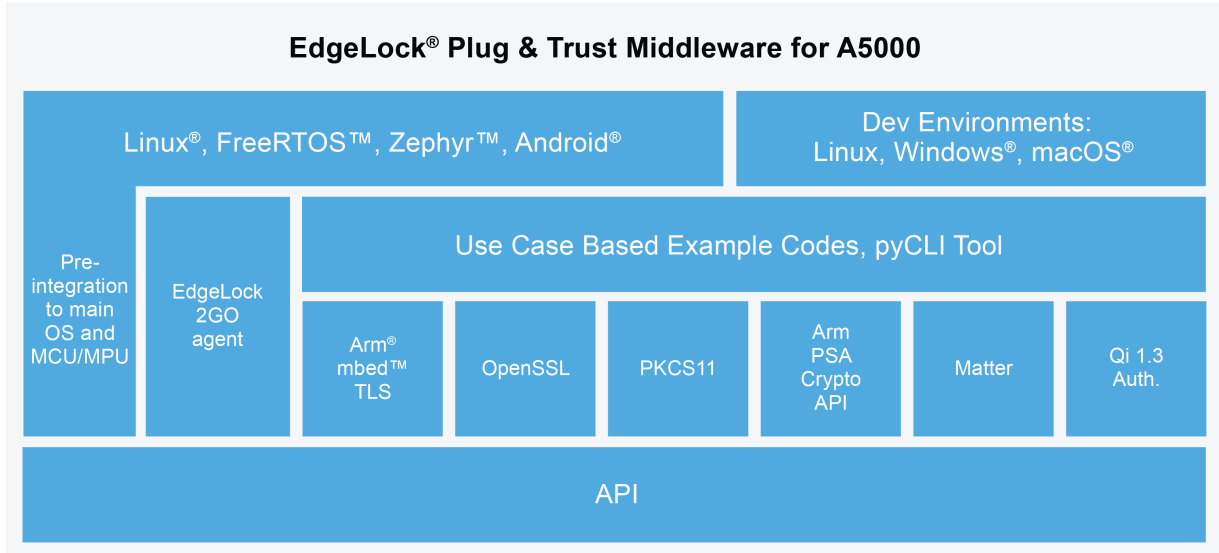
	Name	Description	12NC
	OM-A5000ARD	A5000 Arduino compatible development kit	9354 243 19598 On demand, via NXP eCommerce

Development kit website: www.nxp.com/OM-A5000

5 NXP Board Support Packages and Software

EdgeLock A5000 Plug & Trust Middleware

www.nxp.com/A5000 → Tools & Software



8 Suggested Stocking

The MOQ for the A5000 is 3k. the part is set up in the Q2 pricebook.

For immediate stocking and customer samples we offer you do undergo the MOQ and place a paid sample order at NXP for 100 pieces A5000

Variant	Orderable Part Number	Description	12NC	MOQ	Stocking
A5000	A5000R2HQ1/Z016UZ	EdgeLock secure authenticator with symmetric and asymmetric crypto for authentication use cases	9354 262 25472	3k	100 pc paid sample order

9 Export Compliance

NXP Semiconductors, makes product Export Control Classification Number (ECCN) and Harmonized Tariff Schedule (HTS) classifications available for informational purposes only and the classifications are subject to change without notice. Anyone importing or exporting/re-exporting an NXP item is solely responsible for assuring the ECCN and HTS they use is correct. Further, NXP does not provide guidance regarding the exportability of its products, software or technology. Such questions should be directed to the exporter's internal Trade Compliance organization or legal counsel.

NXP Product Number	USHTS	ECCN	CCATS #	ENC Status	U.S. EAR - Regulatory Reference
A5000R2HQ1/Z016UZ	8542.31 0000	5A992	G158347	n.a.	742.15 (B) (3) (i)

8 Available Documentation

DistyNet → Security and Authentication → Authentication → [EdgeLock Secure Element & Secure Authenticator Portfolio Overview](#)

Data Sheet, etc.: www.nxp.com/A5000

[EdgeLock A5000 Channel Launch Repository](#) *

*Please note that the Channel Launch Repository is for marketing assets like high res block diagram and board photography. This same information is also posted to the "product" launch folder on the distributor extranet for others outside of marketing who may need it.

How to Reach Us

Home Page:

www.nxp.com

Web Support:

www.nxp.com/support

USA/Europe or Locations Not Listed:

NXP Semiconductors
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East and Africa:

NXP Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:

NXP Semiconductors Japan Ltd..
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014
+81 3 5437 9125
support.japan@nxp.com

Asia/Pacific:

NXP Semiconductors Hong Kong Ltd
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright license granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

NXP Semiconductors reserves the right to make changes without further notice to any products herein. NXP Semiconductors makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does NXP Semiconductors assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters which may be provided in NXP Semiconductors data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals" must be validated for each customer application by customer's technical experts. NXP Semiconductors does not convey any license under its patent rights nor the rights of others. NXP Semiconductors products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the NXP Semiconductors product could create a situation where personal injury or death may occur. Should Buyer purchase or use NXP Semiconductors products for any such unintended or unauthorized application, Buyer shall indemnify and hold NXP Semiconductors and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that NXP Semiconductors was negligent regarding the design or manufacture of the part.

