



PRESS RELEASE

September 16, 2026
Ubiquitous AI Corporation

Ubiquitous AI Integrates Post-Quantum Cryptography for IoT Products into Its Security Solution "Ubiquitous Securus," Accelerating Development Toward Commercialization in FY2027

— Combining next-generation cryptography with a security platform proven in mass production to support PQC implementation in embedded products —

Ubiquitous AI Corporation (Headquarters: Shinjuku, Tokyo; President & CEO: Yuta Oyoshi; hereinafter "Ubiquitous AI") today announced that it will integrate post-quantum cryptography (PQC), a key cybersecurity technology, into "Ubiquitous Securus," its tamper-resistant security solution for embedded devices, and will begin offering the security solution required in the era of physical AI from fiscal year 2027.

In anticipation of the practical use of quantum computers, efforts are under way worldwide to migrate today's widely used public-key cryptography to PQC, which can withstand decryption by quantum computers.

Ubiquitous AI has applied the "small, light, and fast" embedded software technology it has cultivated over approximately 25 years to next-generation cryptography, and has been conducting research and development on PQC since 2023. In autumn 2025, the company established the feasibility of PQC implementation on Arm® Cortex®-M-based 32-bit microcontrollers for low-cost IoT products with severe resource constraints. Ubiquitous AI will now integrate this PQC technology into Ubiquitous Securus, its in-house security platform with an extensive track record of adoption in IVI (in-vehicle infotainment) systems and consumer electronics.

Rather than simply providing a PQC-ready cryptographic library, Ubiquitous AI will offer a security solution that combines the functions required for deployment in real-world embedded products, such as secure management and operation of cryptographic keys, protection of encryption/decryption processing, and portability across different SoCs, thereby supporting customers in their phased migration to and implementation of PQC.

About Ubiquitous Securus

Ubiquitous Securus is a tamper-resistant security solution for embedded devices that securely manages confidential information such as cryptographic keys, certificates, and user data, and protects encryption/decryption processing.

In combination with Ubiquitous AI's content protection products "Ubiquitous DTCP" and "Ubiquitous HDCP," Ubiquitous Securus has been widely adopted, mainly in IVI systems and consumer electronics, with approximately 8.4 million units shipped as of September 1, 2026.

Content protection standards such as DTCP and HDCP require strict key management to prevent the leakage of cryptographic keys. To meet these requirements, Ubiquitous Securus provides, in addition to a software cryptographic library, the ability to leverage the hardware encryption/decryption functions built into SoCs, as well as a "Secure Storage" function that securely manages and operates confidential data such as cryptographic keys, certificates, and user data within secure memory spaces such as Arm

TrustZone®.

Furthermore, because the APIs for hardware encryption/decryption functions and the Secure OS running on Arm TrustZone differ depending on the SoC vendor and model, existing development assets may need to be modified when developing derivative or successor models. Ubiquitous Securus provides a wrapper layer that absorbs these differences in SoCs and execution environments, reducing the development workload involved in porting to derivative and successor models without developers having to account for API differences between SoCs.

For encryption/decryption processing as well, Ubiquitous Securus is designed so that either the software library it provides or the hardware encryption/decryption functions of the SoC can be selected according to the environment.

Benefits of Integrating PQC into Ubiquitous Securus

This integration combines next-generation PQC cryptographic algorithms with the capabilities that Ubiquitous Securus has refined through implementation in mass-produced products, such as cryptographic key management and the absorption of hardware differences.

Through this integration, Ubiquitous AI aims to deliver a PQC-ready security solution with the following features:

- Secure management and operation of cryptographic keys
- Prevention of hacking by concealing encryption/decryption processes
- A common API across different SoCs, making it easy to leverage hardware functions
- Smooth switching from software to hardware processing once SoCs support PQC in the future
- Support for hybrid cryptography combining conventional cryptography and PQC, enabling a phased migration to PQC

From R&D to Commercialization: Accelerating the Implementation of "Edge Security 3.0"

Migration to PQC is not completed simply by implementing a cryptographic algorithm once. Particularly for IoT and embedded devices with long product lifecycles, a mechanism that allows the cryptographic schemes in use to be continuously updated in response to future standardization trends, changing threats, and the evolution of hardware environments is essential.

In its medium-term management plan, Ubiquitous AI has positioned security as one of its growth areas, and is advancing the research and development of next-generation security technologies, including PQC, as well as initiatives for their implementation in IoT and embedded devices. (*1)

The "Edge Security 3.0" (*2) concept announced in June 2026 sets out the vision of evolving security beyond an "obligation" for regulatory compliance and risk mitigation into a foundation that supports the value of products and services and enables new business models.

The integration of PQC into Ubiquitous Securus is one of the company's initiatives to bring "Edge Security 3.0" to concrete products, combining PQC, a next-generation cryptographic technology that has until now been developed and offered separately, with device security technology that has a proven track record in mass-produced products.

Ubiquitous AI will continue to contribute to next-generation product security and to enhancing its customers' product competitiveness.

(*1) For details on Ubiquitous AI's PQC initiatives, please see the following:

Appendix: Current Status of Post-Quantum Cryptography (PQC) and Ubiquitous AI's Initiatives (below)

(*2) "Ubiquitous AI Proposes "Edge Security 3.0" Framework, Advancing Next-Generation Security Design

to Drive Value Creation in Embedded Devices — Transforming Security from “Obligation” to “Value Creation” —

URL: <https://www.ubiquitous-ai.com/en/news/2026/005509.html>

Ubiquitous Securus Product Page

URL: <https://www.ubiquitous-ai.com/en/products/securus/>

About Ubiquitous AI Corporation (Tokyo Stock Exchange: 3858)

Ubiquitous AI Corporation delivers advanced technologies and services that support customers in the manufacturing industry, building on decades of experience in embedded software development. With a strong foundation of leading-edge technologies and a global customer base, the company provides proprietary software products alongside related professional services. Ubiquitous AI is committed to the growth of its customers, business partners and society.

Head Office: Shinjuku First West Bldg. 17F, 1-23-7 Nishi-Shinjuku, Shinjuku-ku, Tokyo 160-0023, JAPAN

URL: <https://www.ubiquitous-ai.com/en/>

Note to Investors

This press release is intended to provide information about the qualitative progress of Ubiquitous AI Corporation’s business activities and is not a solicitation for investment. For details regarding financial results, key performance indicators, or forecasts, please refer to our most recent earnings summaries and other disclosures published through the Tokyo Stock Exchange.

Media Contacts

Yu Aso

Marketing and Communication Department, Ubiquitous AI Corporation

+81 3 5908 3451/ <https://www.ubiquitous-ai.com/en/contact/others/>

- The company names and product names mentioned in this news release are the registered trademarks or trademarks of their respective owners.
- The contents of this news release are current as of the date of announcement and are subject to change without notice.

Appendix

Current Status of Post-Quantum Cryptography (PQC) and Ubiquitous AI's Initiatives

Current Status of Post-Quantum Cryptography (PQC)

In anticipation of the practical use of quantum computers, there is a global movement to migrate widely used public-key cryptography, such as RSA and elliptic curve cryptography, to PQC, a cryptographic approach that can withstand decryption by quantum computers.

In 2024, NIST (the U.S. National Institute of Standards and Technology) established "FIPS 203 (ML-KEM)," "FIPS 204 (ML-DSA)," and "FIPS 205 (SLH-DSA)" as the principal PQC standards. In 2025, NIST selected "HQC," which is based on a different mathematical foundation from "ML-KEM," for standardization as an additional key-establishment mechanism, and is also advancing the standardization of "FN-DSA," based on "FALCON," as "FIPS 206."

PQC is moving from the research and evaluation stage to the implementation and migration stage. However, for IoT and embedded devices, which have limited CPU, memory, storage, and other resources compared with servers and PCs, migration to PQC, with its high implementation burden, is only now beginning in earnest. In addition, IoT and embedded devices have long lifecycles, and changing their cryptographic schemes after shipment is not easy. For future embedded devices, therefore, it will be important not only to implement PQC algorithms but also to have mechanisms such as the following:

- The ability to select cryptographic schemes according to product characteristics and security requirements
- Support for transitional configurations that combine conventional cryptography and PQC
- The ability to switch cryptographic schemes in response to future standardization and changing threats
- Secure management and operation of cryptographic keys, certificates, and other assets
- Management of certificates in line with the product lifecycle, even after shipment

NIST also identifies cryptographic asset visibility (understanding existing cryptographic usage), risk management, and the interoperability and performance evaluation of products and services incorporating PQC as important themes in PQC migration.

Ubiquitous AI's PQC Initiatives

Since 2023, Ubiquitous AI has been engaged in PQC research and development, building an understanding of algorithm specifications in light of NIST standardization trends, developing its own implementations, and conducting comparative verification against reference implementations.

In November 2025, the company completed the implementation and verification of the NIST-standardized "FIPS 203," "FIPS 204," and "FIPS 205" on low-cost Arm® Cortex®-M-based 32-bit microcontrollers. It is also advancing implementations of "FALCON" and "HQC," which were then still undergoing standardization, based on the specifications available at the time.

In June 2026, the company announced its "Edge Security 3.0" concept. Rather than offering a standalone PQC library, the company is integrating PQC into "Ubiquitous Securus," its tamper-resistant security solution for embedded devices, and applying it to its TLS encrypted communications library, positioning PQC as a next-generation security technology that can be implemented even on highly resource-constrained embedded devices.

Building on the results of its research and development to date, Ubiquitous AI will now evolve PQC from a standalone cryptographic algorithm into a security platform that encompasses encrypted communications, device protection, key management, and even product lifecycle management.

1. Support for a Range of Cryptographic Algorithms

Ubiquitous AI aims to build a flexible cryptographic platform that is not tied to any specific cryptographic algorithm, taking into account the applications, resources, security requirements, and product lifecycles of embedded devices.

Category	Algorithm	Approach
PQC / Key establishment	ML-KEM (FIPS 203)	Promoting implementation in embedded devices and commercialization as the primary supported scheme.
	HQC	Continuously tracking standardization trends as a backup scheme and considering support in products.
PQC / Digital signature	ML-DSA (FIPS 204)	Promoting support as the primary signature scheme.
	SLH-DSA (FIPS 205)	Supported as a backup scheme based on a different mathematical foundation.
	FN-DSA (FALCON)	Considering support, including for resource-constrained embedded devices, in light of standardization trends.
Conventional / Symmetric key	AES, DES, etc.	Ciphers with sufficient key lengths, such as AES-256, will continue to be used as important foundational technologies even after the migration to PQC. Longer key lengths can also be supported as needed.
Conventional / Public key	RSA, ECC, etc.	Used together with PQC in consideration of the migration period, supporting a phased transition.

Ubiquitous AI aims to provide an environment in which appropriate cryptographic schemes can be selected and changed according to a product's security requirements, performance, memory capacity, communication method, product lifecycle, and other factors, avoiding rigid dependence on any specific cryptographic algorithm.

2. Integration into "Ubiquitous Securus," a Tamper-Resistant Security Solution for Embedded Devices

By integrating PQC into "Ubiquitous Securus," rather than only providing a PQC-ready cryptographic library, Ubiquitous AI can offer a security solution that combines the functions required for deployment in actual embedded products.

Through this integration, Ubiquitous AI is working to deliver a PQC-ready security solution with the following features:

- Secure management and operation of cryptographic keys (Secure Storage function)
- Prevention of hacking by concealing encryption/decryption processes
- A common API across different SoCs, making it easy to leverage hardware functions (encryption/decryption and memory protection)
- Smooth switching from software processing to hardware processing once SoCs support PQC in the future
- Support for hybrid cryptography combining conventional cryptography and PQC, enabling a phased migration to PQC

Migration to PQC is not completed simply by implementing a cryptographic algorithm once. Particularly for IoT and embedded devices with long product lifecycles, a mechanism that allows the cryptographic schemes in use to be continuously updated in response to future standardization trends, changing threats, and the evolution of hardware environments is essential.

In its medium-term management plan, Ubiquitous AI has positioned security as one of its growth areas, and is advancing the research and development of next-generation security technologies, including PQC, as well as initiatives for their implementation in IoT and embedded devices.