**News Release**

No.: REN2218(A)

**Renesas RA Family MCUs Achieve CAVP Certification for Comprehensive Suite of Cryptographic Algorithms**

*RA Family of 32-bit Arm Cortex-M Microcontrollers Offers Ultimate IoT Security with Renesas’s Secure Crypto Engine (SCE) and Arm TrustZone*

**Düsseldorf, May 17, 2022 ―** Renesas Electronics Corporation (TSE:6723), a premier supplier of advanced semiconductor solutions, today announced that the security engine of its RA Family of 32-bit Arm® Cortex®-M microcontrollers (MCUs) has been certified by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Verification Program (CAVP). The drivers to utilize the certified SCE9 Protected Mode are included in the RA Family Flexible Software Package (FSP) v3.6.0 and later.

The Renesas RA6M4, RA6M5, RA4M2, and RA4M3 MCU Groups all received NIST CAVP certification of a comprehensive suite of cryptographic algorithms, including multiple modes of Advanced Encryption Standard (AES), hashing, Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) key generation and authentication, Key Agreement Schemes, and Deterministic Random Bit Generator (DRBG). NIST CAVP certification provides independent verification of the correct implementation of the cryptographic algorithms, which is vital to ensure connectivity interoperability.

Renesas announced last year that RA devices received both PSA Certified Level 2 and Security Evaluation Standard for IoT Platforms (SESIP) certifications.

“With CAVP certification, in conjunction with the existing SESIP1 and PSA Certified Level 2, Renesas provides the industry’s most comprehensive IoT security solutions,” **said Roger Wendelken, Senior Vice President in Renesas’ IoT and Infrastructure Business Unit**. “Customers in a broad range of connected application segments can implement the RA family with supreme confidence that their data will be secure.”

Renesas’ unique integrated security architecture provides a time and energy-efficient solution with unlimited secure key storage. An independent evaluation to compare SCE9 Protected Mode operation to a selection of industry-leading secure elements was recently completed. “The SCE9 doesn't just pack a significant amount of cryptographic compute power, but getting rid of a serial interface (usually I2C) to an externally connected device provides various advantages, said **Mario Noseda from Zurich University of Applied Sciences, School of Engineering**. “The high clock frequency of the internal data bus greatly reduces the data transmission time between the MCU and the SCE9. But even more important is the complete elimination of a point of attack, which is a huge selling point for an MCU containing the SCE9.”

Proper handling of cryptographic keys is vital to maintaining the integrity of a secure product. The new Security Key Management Tool provides a straight-forward mechanism for preparing keys for secure installation and updates, supporting development, production provisioning, and key updates for products in the field. The GUI interface is designed to assist developers, particularly those new to security solutions, to create prototypes and proofs-of concepts with test keys. The command line interface coordinates across multiple developers and supports production key management of key provisioning and update. Downloadable Application Projects demonstrate how to perform secure key installation and updates for both development and production using the available Renesas tools. Find the complete list of security-orientated software, tools, and solutions at [www.renesas.com/iot-security](http://www.renesas.com/iot-security).

In addition to these widely recognized industry certifications, Renesas RA MCUs offer customers the ultimate IoT security by combining Secure Crypto Engine IP with NIST CAVP certifications on top of Arm TrustZone® for Armv8-M. RA Family devices incorporate hardware-based security features from simple AES acceleration to fully-integrated crypto subsystems isolated within the MCU. The Secure Crypto Engine provides symmetric and asymmetric encryption and decryption, hash functions, true random number generation (TRNG), and advanced key handling, including key generation and MCU-unique key wrapping. An access management circuit shuts down the crypto engine if the correct access protocol is not followed, and dedicated RAM ensures that plaintext keys are never exposed to any CPU or peripheral bus.

**About Renesas’ RA MCU Family**

The RA Family ecosystem accelerates the development of IoT applications with core technologies such as security, safety, connectivity and HMI. Designing with RA MCUs makes it easy for engineers to develop Internet of Things (IoT) endpoint and edge devices for industrial and building automation, metering, healthcare, and home appliance applications.  The RA Family includes the RA2 Series (up to 48 MHz), RA4 Series (up to 100 MHz), RA6 Series (up to 240 MHz), and the single/dual-core RA8 Series, to be released later. More information about the RA MCU Family is available at [www.renesas.com/RA](http://www.renesas.com/RA).

**About Renesas Electronics Corporation**

Renesas Electronics Corporation ([TSE: 6723](http://www.jpx.co.jp/english/)) empowers a safer, smarter and more sustainable future where technology helps make our lives easier. A leading global provider of microcontrollers, Renesas combines our expertise in embedded processing, analog, power and connectivity to deliver complete semiconductor solutions. These Winning Combinations accelerate time to market for automotive, industrial, infrastructure and IoT applications, enabling billions of connected, intelligent devices that enhance the way people work and live. Learn more at [renesas.com](http://www.renesas.com/). Follow us on [LinkedIn](https://www.linkedin.com/company/renesas/), [Facebook](https://www.facebook.com/RenesasElectronics/), [Twitter](https://twitter.com/renesasglobal), [YouTube](https://www.youtube.com/user/RenesasPresents), and [Instagram](https://www.instagram.com/renesas_global/).

###

(Remarks) Arm, Arm Cortex, and Arm TrustZone are trademarks or registered trademarks of Arm Limited in the EU and other countries. All names of products or services mentioned in this press release are trademarks or registered trademarks of their respective owners.

**Media contact for further information, text and graphics or to discuss feature article opportunities:**

Alexandra Janetzko / Martin Stummer

HBI Helga Bailey GmbH (PR agency), Stefan-George-Ring 2, 81929 Munich, Germany

Tel.: +49 89 99 38 87-32 / -34

Email: alexandra\_janetzko@hbi.de / martin\_stummer@hbi.de

Web: [www.hbi.de](http://www.hbi.de/)