1. **Communiqué de presse**

No. : REN2218(A)

**Les Microcontrôleurs de la Famille RA de Renesas Obtiennent la Certification CAVP pour une Suite Complète d'Algorithmes Cryptographiques**

*La Famille RA de Microcontrôleurs Arm Cortex-M 32 Bits Offre une Sécurité IoT Ultime avec le Secure Crypto Engine (SCE) de Renesas et la TrustZone d’Arm*

**Düsseldorf, le 19 mai 2022 ―** Renesas Electronics Corporation (TSE : 6723), l'un des principaux fournisseurs de solutions avancées de semi-conducteurs, a annoncé aujourd'hui que le moteur de sécurité de sa famille RA de microcontrôleurs (MCU) Arm® Cortex®-M 32 bits a été certifié par le National Institute of Standards and Technology (NIST) Programme de Vérification des Algorithmes Cryptographiques (CAVP). Les pilotes permettant d'utiliser le mode protégé du SCE9 certifié sont inclus dans le package logiciel flexible (FSP) v3.6.0 et versions ultérieures de la famille RA.

Les groupes de MCU RA6M4, RA6M5, RA4M2 et RA4M3 de Renesas ont tous reçu la certification NIST CAVP d'une suite complète d'algorithmes cryptographiques, y compris plusieurs modes d’Avanced Encryption Standard (AES), de hachage, de Rivest Shamir Adleman (RSA) et de génération et authentification de clé par cryptographie à courbe elliptique (ECC), schémas d'accord de clé et générateur de bits aléatoires déterministes (DRBG). La certification NIST CAVP fournit une vérification indépendante de la mise en œuvre correcte des algorithmes cryptographiques, ce qui est essentiel pour assurer l'interopérabilité de la connectivité.

Renesas a annoncé l'année dernière que les composants RA avaient reçu les certifications PSA Certified Level 2 et Security Evaluation Standard for IoT Platforms (SESIP).

« Avec la certification CAVP, en conjonction avec les certifications SESIP1 et PSA Level 2 existantes, Renesas fournit les solutions de sécurité IoT les plus complètes du secteur », **a déclaré Roger Wendelken, vice-président senior de l'unité commerciale IoT et Infrastructure de Renesas**. « Les clients d'un large éventail de segments d'applications connectées peuvent mettre en œuvre la famille RA avec la certitude absolue que leurs données seront sécurisées. »

L'architecture de sécurité intégrée unique de Renesas fournit une solution économe en temps et en énergie avec un stockage de clés sécurisé illimité. Une évaluation indépendante visant à comparer le fonctionnement du SCE9 en mode protégé à une sélection d'éléments sécurisés de pointe a été récemment achevée. « Le SCE9 ne contient pas seulement une quantité importante de puissance de calcul cryptographique, mais se débarrasser d'une interface série (généralement I2C) vers un appareil connecté en externe offre divers avantages », **a déclaré Mario Noseda de l'Université des Sciences Appliquées de Zurich, École d'Ingénierie**. « La fréquence d'horloge élevée du bus de données interne réduit considérablement le temps de transmission des données entre le MCU et le SCE9. Mais encore plus important est l'élimination complète d'un point d'attaque, qui est un énorme argument de vente pour un MCU contenant le SCE9. »

Un livre blanc détaillant l'évaluation est disponible ici [htpps://digitalcollection.zhaw.ch/bitstream/11475/23809/3/2021\_Noseda-Ruest\_Crypto-acceleration-for-IoT.pdf](https://digitalcollection.zhaw.ch/bitstream/11475/23809/3/2021_Noseda-Ruest_Crypto-acceleration-for-IoT.pdf?utm_campaign=mcu_ra_security&utm_source=press_release&utm_medium=press_release&utm_content=wp).

Une bonne gestion des clés cryptographiques est essentielle pour maintenir l'intégrité d'un produit sécurisé. Le nouvel outil de gestion des clés de sécurité fournit un mécanisme simple pour préparer les clés pour une installation et des mises à jour sécurisées, prendre en charge le développement, la configuration pour la production et les mises à jour des clés pour les produits sur le terrain. L'interface graphique est conçue pour aider les développeurs, en particulier ceux qui découvrent les solutions de sécurité, à créer des prototypes et des preuves de concepts avec des clés de test. L'interface de ligne de commande assure la coordination entre plusieurs développeurs et prend en charge la gestion des clés de production pour la configuration et la mise à jour des clés. Les projets d'application téléchargeables montrent comment effectuer une installation et des mises à jour sécurisées des clés pour le développement et la production à l'aide des outils Renesas disponibles. Retrouvez la liste complète des logiciels, outils et solutions orientés sécurité sur [www.renesas.com/iot-security](http://www.renesas.com/iot-security).

En plus de ces certifications largement reconnues dans l'industrie, les microcontrôleurs RA de Renesas offrent aux clients la sécurité IoT ultime en combinant le Secure Crypto Engine avec les certifications NIST CAVP en plus de la TrustZone® d’Arm pour Armv8-M. Les composants de la famille RA intègrent des fonctionnalités de sécurité matérielles allant de la simple accélération AES aux sous-systèmes de chiffrement entièrement intégrés et isolés dans le MCU. Le Secure Crypto Engine fournit un chiffrement et un déchiffrement symétriques et asymétriques, des fonctions de hachage, une génération de nombres aléatoires véritables (TRNG) et une gestion avancée des clés, y compris la génération de clés et l'encapsulation de clé unique au MCU. Un circuit de gestion des accès arrête le moteur de cryptage si le protocole d'accès correct n'est pas suivi, et une RAM dédiée garantit que les clés en clair ne sont jamais exposées à un processeur ou à un bus périphérique.

**À propos de la famille de MCU RA de Renesas**

L'écosystème de la famille RA accélère le développement d'applications IoT avec des technologies de base telles que la sécurité, la sûreté, la connectivité et l'IHM. La conception avec des microcontrôleurs RA permet aux ingénieurs de développer facilement des dispositifs de périphérie de l'Internet des objets (IoT) pour les applications d'automatisation industrielle et de bâtiment, de comptage, de soins de santé et d'appareils électroménagers. La famille RA comprend la série RA2 (jusqu'à 48 MHz), la série RA4 (jusqu'à 100 MHz), la série RA6 (jusqu'à 240 MHz) et la série RA8 simple/double cœur, qui sortira plus tard. Plus d'informations sur la famille de MCU RA sont disponibles sur [www.renesas.com/RA](http://www.renesas.com/RA).

**À propos de Renesas Electronics Corporation**

Renesas Electronics Corporation ([TSE: 6723](http://www.jpx.co.jp/english/)) offre un avenir plus sûr, plus intelligent et plus durable où la technologie nous facilite la vie. L'un des principaux fournisseurs mondiaux de microcontrôleurs, Renesas combine notre expertise dans le traitement embarqué, l'analogique, l'alimentation et la connectivité pour fournir des solutions complètes de semi-conducteurs. Ces combinaisons gagnantes accélèrent la mise sur le marché des applications automobiles, industrielles, d'infrastructure et IoT, permettant à des milliards d'appareils connectés et intelligents d'améliorer la façon dont les gens travaillent et vivent. En savoir plus sur [renesas.com](http://www.renesas.com/). Suivez-nous sur [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) et [Instagram](https://www.instagram.com/renesas_global/).

###

(Remarques) Arm, Arm Cortex et Arm TrustZone sont des marques ou des marques déposées d'Arm Limited dans l'UE et dans d'autres pays. Tous les noms de produits ou services mentionnés dans ce communiqué de presse sont des marques ou des marques déposées de leurs propriétaires respectifs.

**Contact médias :**

Alexandra Janetzko

HBI Helga Bailey GmbH (PR agency)

Tel.: +49 89 99 38 87-32

Email: [alexandra\_janetzko@hbi.de](mailto:alexandra_janetzko@hbi.de)

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