

Renesas Electronics and ESCRYPT Collaborate on State-of-the-Art Combined Hardware/Software Solution with High-Level Security for Protecting Automotive ECUs

New Platform Solution Facilitates Security Integration in Complex Automotive Applications for the Autonomous Driving Era

TOKYO, Japan, BOCHUM, Germany, November 24, 2016 — Renesas Electronics Corporation, a premier supplier of advanced semiconductor solutions, and ESCRYPT GmbH (“ESCRYPT”), a leading system provider for embedded security, announce their collaboration on an integrated hardware and software platform solution that provides high-level security for protecting automotive electronic control units (ECUs).

The new joint hardware/software platform solution comprises Renesas' RH850/P1x-C Series of automotive safety microcontrollers (MCUs) that combine on a single-chip: functional safety, security, and vehicle control network technologies, with ESCRYPT's CycurHSM, a security software stack, to realize highly complex automotive security solutions. The new solution reduces development time and integrates security functions in safety-critical automotive ECU applications. Additionally, the solution serves as a stepping stone to achieve autonomous driving by accelerating the integration of safety and security functions.

In the autonomous driving era, in-vehicle infotainment, vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) networks are expected to become mainstream. The connectivity between these networks allows systems to obtain information on road conditions and other factors that could impact the driving experience. It also requires robust security measures to ensure the systems are protected from unauthorized external access.

The RH850/P1x-C Series integrates a hardware security module with a co-processor supporting data encryption, authentication, and random number generation to address these mission-critical security requirements in vehicle systems. CycurHSM is a security software stack that perfectly fits RH850/P1x-C MCUs and complements the security features in hardware with additional security services, e.g., secure boot, secure flashing, and debugging.

New use cases such as software updates Over-the-Air (SOTA/FOTA) or advanced driver assistance systems (ADAS) and the resulting in-vehicle communications require higher ECU protection levels against unauthorized or malicious access and manipulation. Therefore, in addition to protection software, hardware security protection within the ECU has also become essential.

The globally available combination of Renesas and ESCRYPT products enhances security of connected, highly-automated vehicles, provides high value, and solves these security problems.

Key features of the combined hardware/software platform solution:

(1) Combined solution accelerates safety and security functions required for vehicles of the autonomous era with highly optimized HSM technology

The combined hardware/software solution comprises of Renesas' 40 nanometer (nm) automotive RH850/P1x-C on-chip hardware security module (HSM), the ICU-M (Note 1), as well as ESCRYPT's highly optimized software that ensures the highest level of ECU security.

The ICU-M provides security services based on private and public key cryptography that allow advanced cyber-security use case implementations. The ICU-M includes dedicated secure code/data flash, enhanced debug control methods by dynamic authentication, fast AES (Note 2) engine with multiple execution contexts and complex ciphering modes, pseudo random number generation seeded by true random number generator compliant with AIS-31 (Note 3), and many other security features.

CycurHSM is a scalable solution, ranging from SHE (Note 4) and SHE+ up to full HSM functionality (such as secure flashing, secure onboard communication, advanced mechanisms for secure boot, secure debugging, or feature activation). CycurHSM runs on the ICU-M and provides dedicated software interfaces to make use of the full power of HSM technology. ESCRYPT's HSM security stack will be available for further Renesas MCUs in the near future.

(2) Significantly reducing development and implementation time by up to 90 percent by simplifying implementation of security functions

ECU developers can rely on optimal-fit components from Renesas and ESCRYPT to simplify implementation of the desired security functions. For an existing AUTOSAR application, since the combined hardware/software solution is fully AUTOSAR-compliant, no further development of security functions is required and the remaining tasks boil down to a simple configuration of the software, thereby eliminating up to 90 percent of the development effort.

For new applications, AUTOSAR-compliant or not, the clean interface offered by the combined hardware/software enables system developers to concentrate on high-level software development, without having to worry about low-level or hardware-specific issues. This leads to a significant reduction of the overall effort by at least 50 percent in case of new applications.

(3) Additional security services available to further optimize security functions that add value to highly autonomous vehicles

The security solution can be further enriched by additional security services such as risk analysis and efficient security concepts, as well as software products such as key management from ESCRYPT. The security solution can also be integrated into a full AUTOSAR stack, as e.g., provided by ESCRYPT's parent company ETAS.

The jointly-developed platform solution is a turnkey, high-quality solution covering a wide field of hardware and software aspects – delivered by two automotive expert players. Security and performance levels mandated by new automotive use cases can be reached to avoid remote hacking and various security issues – by a complete hardware and software approach through the combined expertise of Renesas and ESCRYPT.

The globally available combination of Renesas and ESCRYPT products will enhance the security of connected, highly automated vehicles and provide added value to customers worldwide.

Availability

The jointly-developed integrated hardware and software platform solution is now available. (Availability is subject to change without notice.)

(Note 1) A hardware security module developed by Renesas equipping a co-processor, which can encrypt/decrypt data and generate a random number.

(Note 2) AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).

(Note 3) AIS-31 is a paper that defines a non-deterministic random number generator.

(Note 4) SHE (Secure Hardware Extension) is an industrial standard that describes a small hardware extension for adding essential security functionality.

About Renesas Electronics Corporation

Renesas Electronics Corporation ([TSE: 6723](#)) delivers trusted embedded design innovation with complete semiconductor solutions that enable billions of connected, intelligent devices to enhance the way people work and live – securely and safely. The number one global supplier of microcontrollers and a leader in Analog & Power and SoC products, Renesas provides the expertise, quality, and comprehensive solutions for a broad range of Automotive, Industrial, Home Electronics (HE), Office Automation (OA), and Information Communication Technology (ICT) applications to help shape a limitless future.

Learn more at [renesas.com](https://www.renesas.com)

About ESCRYP T – Embedded Security

ESCRYP T – Embedded Security is the leading system provider for embedded security worldwide. With locations in Germany, the UK, Sweden, the USA, Canada, China, Korea, and Japan we have security specialists available to help with current security topics such as secure M2M-communication, IT security in the Internet of Things, protection of e-business models, and automotive security and they develop highly secure, worldwide valued products and solutions which are tailored to the specific requirements of embedded systems and the relevant IT infrastructure and are tested and proven a million times in automotive series production. ESCRYP T is a subsidiary of ETAS GmbH, a wholly owned subsidiary of the Bosch Group.

www.escrypt.com

###

(Remarks) All registered trademarks or trademarks are the property of their respective owners.

Media contact Germany:

ESCRYP T GmbH

Bianka Ansperger

Marketing Manager

+49 234 43870-213

bianka.ansperger@escrypt.com

Media contact Japan:

Renesas Electronics Corporation

Kyoko Okamoto

+ 81-3-6773-3001

kyoko.okamoto.sx@renesas.com