**Renesas Electronics und ESCRYPT kooperieren zu hochmoderner kombinierter Hard-/Softwarelösung für High-Level-Security bei Automotive-Steuergeräten**

***Neue Plattformlösung für einfachere Security-Integration bei komplexen Automotive-Anwendungen für das autonome Fahren***

**TOKIO (Japan), BOCHUM, 24. November 2016 —** Renesas Electronics Corporation, ein führender Hersteller hochmoderner Halbleiterlösungen, und die ESCRYPT GmbH – Embedded Security („ESCRYPT“), das führende Systemhaus für eingebettete IT-Sicherheit, geben die gemeinsame Arbeit an einer integrierten Hard- und Softwareplattform für High-Level-Security von Automotive-Steuergeräten (ECUs) bekannt.

Bei der neuen kombinierten Hard-/Softwareplattform werden die automotive Safety-Mikrocontroller (MCUs) der RH850/P1x-C-Reihe von Renesas, welche funktionale Sicherheit, Security und Netzwerktechnologien auf einem Chip vereinen, mit ESCRYPTs Security-Software-Stack für Hardware-Security-Module, CycurHSM, verbunden. Hierdurch werden hochkomplexe Security-Lösungen für Fahrzeuge ermöglicht und Entwicklungszeiten verkürzt. Zudem wirkt sie als Beschleuniger des autonomen Fahrens, indem sie es ermöglicht, die erforderlichen Safety- und Security-Funktionen schneller zu verwirklichen. In autonomen Fahrzeugen werden Infotainmentsysteme, Fahrzeug-zu-Fahrzeug-Kommunikation (V2V) und Fahrzeug-zu-Infrastruktur-Netzwerke (V2I) allgegenwärtig sein. Durch die Verknüpfung dieser Netzwerke werden Informationen über die Straßenbedingungen und andere sicherheitsrelevante Daten, die das Fahrverhalten beeinflussen können, ausgetauscht. Dementsprechend ist es wichtig, die Systeme mit Hilfe von massiven Sicherheitsmaßnahmen vor unerlaubten Zugriffen von außen zu schützen.

Die RH850/P1x-C-Reihe erfüllt die wesentlichen Sicherheitsanforderungen in Fahrzeugsystemen, indem sie ein Hardware-Security-Modul (HSM) mit einem Co-Prozessor verbindet, der Datenverschlüsselung, -authentifizierung und die Berechnung von Zufallszahlen unterstützt. Der Security-Software-Stack CycurHSM passt optimal zu RH850/P1x-C-MCUs und ergänzt die hardwarebasierten Sicherheitsfunktionen mit zusätzlichen Security-Services wie sicherem Booten, Flashen und Debuggen.

Doch auch vor der Einführung absolut autonom fahrender Verkehrsmittel machen neue Anwendungsfälle wie Software-Updates Over-the-Air (SOTA/FOTA) und fortschrittliche Fahrerassistenzsysteme (ADAS) und die daraus resultierende Kommunikation im Fahrzeug

eine höhere ECU-Sicherheit erforderlich, um das Fahrzeugsystem vor unerwünschten Zugriffen und Manipulationen zu bewahren. Daher sind neben Schutzsoftware auch heute schon hardwarebasierte Security-Systeme in der ECU wichtig.

Die weltweit verfügbare Kombination aus Produkten von Renesas und ESCRYPT verbessert die Sicherheit vernetzter, hochautomatisierter Fahrzeuge, bietet Mehrwerte und löst die genannten Sicherheitsprobleme.

**Hauptmerkmale der kombinierten Hard-/Softwareplattform:**

**(1) <u>Kombinierte Lösung mit hochoptimierter HSM-Technologie für schnellere Safety- und Security-Funktionen für das autonome Fahren</u>**

Die kombinierte Hard-/Softwarelösung umfasst das On-Chip-HSM RH850/P1x-C, das im 40-nm-Automotive-Prozess gefertigt wird, die ICU-M (Anm. 1) und hochoptimierte Software von ESCRYPT, die höchstmögliche ECU-Sicherheit gewährleistet.

Die ICU-M stellt Security-Services bereit, die auf Kryptographie mit privaten und öffentlichen Schlüsseln basieren und die Umsetzung von Anwendungsfällen für fortschrittliche Cyber-Security ermöglichen. Die ICU-M umfasst einen dedizierten sicheren Code- und Flash-Datenspeicher, verbesserte Methoden für die Debug-Steuerung durch dynamische Authentifizierung, eine schnelle AES-Engine (Anm. 2) mit mehreren Ausführungskontexten und komplexen Chiffriermodi, die Erzeugung von Pseudozufallszahlen, die durch einen Generator für echte Zufallszahlen gemäß AIS-31 (Anm. 3) initialisiert werden, und viele weitere Security-Funktionen.
CycurHSM ist von SHE (Anm. 4) über SHE+ bis hin zu voller HSM-Funktionalität (darunter sicheres Flashen, sichere Onboard-Kommunikation, hochentwickelte Mechanismen für sicheres Booten, sicheres Debuggen oder Funktions-Freischaltungen) skalierbar. CycurHSM läuft auf der ICU-M und stellt dedizierte Softwareschnittstellen für die optimale Nutzung der HSM-Technologie bereit. Der HSM-Security-Stack von ESCRYPT wird in naher Zukunft auch für weitere MCUs von Renesas verfügbar sein.

**(2) <u>Bis zu 90 % schnellere Entwicklung und Implementierung durch einfachere Umsetzung von Security-Funktionen</u>**

Renesas und ESCRYPT stellen ECU-Entwicklern maßgeschneiderte Komponenten bereit, die die Implementierung der gewünschten Security-Funktionen vereinfachen. Da die kombinierte Hard-/Softwarelösung vollständig AUTOSAR-konform ist, müssen für bestehende AUTOSAR-Anwendungen keine weiteren Security-Funktionen entwickelt

werden, sondern lediglich die Software konfiguriert werden. Dies senkt den Entwicklungsaufwand um bis zu 90 %.

Durch die klar definierte Schnittstelle der kombinierten Hard-/Softwarelösung können sich Entwickler neuer Anwendungen auf die Entwicklung von High-Level-Software konzentrieren und müssen sich nicht um Low-Level- oder hardwarespezifische Probleme kümmern. Das gilt sowohl für AUTOSAR-konforme als auch für nicht-AUTOSAR-konforme Software. Dadurch sinkt der Gesamtaufwand bei neuen Anwendungen um mindestens 50 %.

**(3) <u>Verfügbarkeit zusätzlicher Security-Services zur weiteren Optimierung von Security-Funktionen, die Mehrwerte für hochautonome Fahrzeuge bieten</u>**

Die Security-Lösung lässt sich durch Security-Services wie Risikoanalyse und effiziente Security-Konzepte sowie durch Softwareprodukte wie das Schlüsselmanagement von ESCRYPT erweitern. Die Lösung kann zudem in vollständige AUTOSAR-Stacks integriert werden, wie sie z. B. von ETAS, der Muttergesellschaft von ESCRYPT, angeboten werden.

Die gemeinsam entwickelte Plattform ist eine hochwertige, schlüsselfertige Lösung zweier Automobil-Spezialisten, die verschiedenste Hardware- und Softwareaspekte abdeckt. Da die Lösung Sicherheits- und Leistungsanforderungen erfüllt, die mit neuen Automotive-Anwendungsfällen einhergehen, lassen sich Hackerangriffe und andere Sicherheitsprobleme vermeiden. Hierfür bündeln Renesas und ESCRYPT ihr Know-how in einer umfassenden Hard- und Softwarelösung.

Die weltweit verfügbare Kombination aus Produkten von Renesas und ESCRYPT verbessert künftig die Security vernetzter, hochautomatisierter Fahrzeuge und bietet Kunden weltweit Mehrwerte.

**Verfügbarkeit**
Die gemeinsam entwickelte integrierte Hard- und Softwareplattform ist ab sofort verfügbar (Änderungen vorbehalten).

(Anm. 1) ICU-M ist ein von Renesas entwickeltes HSM mit Co-Prozessor, der Daten ver- und entschlüsseln und Zufallszahlen erzeugen kann.

(Anm. 2) AES ist ein Verschlüsselungsverfahren des US-amerikanischen National Institute of Standards and Technology (NIST) für elektronische Daten.

(Anm. 3) Das AIS-31-Dokument definiert einen nicht-deterministischen Zufallszahlengenerator.

(Anm. 4) SHE (Secure Hardware Extension) ist eine Industrienorm, die von der Herstellerinitiative Software (HIS) definiert wurde und beschreibt eine kostengünstige Hardware-Erweiterung für essentielle Security-Funktionalitäten.

**Über Renesas Electronics Europe**
Renesas liefert mit seinen umfassenden Halbleiterlösungen innovatives Embedded Design. Als weltweite Nummer eins im Markt für Mikrocontroller und einer der führenden Anbieter von A&P- und SoC-Produkten steht Renesas für langjährige Expertise und höchste Qualität. Mit seiner breiten Lösungspalette fokussiert Renesas auf die Anwendungsbereiche Automotive, Industrie, Smart Home, Büroautomation sowie Informations- und Kommunikationstechnologie. Das im Jahr 2010 gegründete Unternehmen hat seinen Hauptsitz in Japan. Mit mehr als 800 Hardware- und Software-Alliance-Partnern weltweit verfügt das Unternehmen über das größte lokale Support-Netzwerk der Branche. Die europäische Firmenstruktur besteht aus den zwei Geschäftsbereichen Automotive und Industrial sowie der globalen ADAS Solutions Group und der Engineering Group.

Weitere Informationen unter: www.renesas.com

Renesas Electronics Europe informiert auch auf http://twitter.com/Renesas_Europe, http://facebook.com/RenesasEurope und http://youtube.com/RenesasPresents.

**Über ESCRYPT – Embedded Security**

ESCRYPT – Embedded Security ist das führende Systemhaus für eingebettete IT-Sicherheit. An Standorten in Deutschland, Großbritannien, Schweden, den USA, Kanada, China, Korea und Japan konzentrieren sich unsere Experten auf aktuelle Datensicherheitsthemen wie sichere M2M-Kommunikation, IT-Sicherheit im Internet der Dinge, Absicherung von E-Business-Modellen und Automotive Security. Hierzu entwickeln sie hochsichere, weltweit geschätzte Security-Produkte und -Lösungen, die speziell auf die Anforderungen von Embedded Systemen und der relevanten IT-Infrastruktur zugeschnitten sind und die sich bereits in der automobilen Serienproduktion millionenfach bewährt haben.

ESCRYPT ist ein Tochterunternehmen der ETAS GmbH, einer hundertprozentigen Tochtergesellschaft der Bosch-Gruppe.

www.escrypt.com

###



**Medienkontakt Deutschland:**
ESCRYPT GmbH
Bianka Ansperger
Marketing Manager
+49 234 43870-213
bianka.ansperger@escrypt.com

**Medienkontakt Japan:**
Renesas Electronics Corporation
Kyoko Okamoto
+ 81-3-6773-3001
kyoko.okamoto.sx@renesas.com