瑞萨科技开发用于信用卡/借记卡和身份证等智能卡的RS-4系列增强性能16位安全MCU

-- 五倍于瑞萨较早MCU的性能，有助于实现高级别安全应用所需的出众性能和功能的接触式或非接触式智能卡 --

东京，2007年11月12日——瑞萨科技公司（Renesas Technology Corp.）今天宣布，开发出用于需要高级别安全性智能卡应用领域的新的RS-4系列16位安全MCU*[1]，这些应用包括银行或信贷公司发出的信用卡或借记卡和身份证。RS-4系列可以实现以前瑞萨同类产品五倍的处理性能。预计该系列的第一款产品将于2008年第二季度（4月至6月）发布。

新的RS-4系列16位安全MCU是AE-4系列16位安全MCU的后续产品，它拥有骄人的成功记录。RS-4系列保持了与其上一代产品的CPU指令代码的兼容，而且可以实现大约五倍*[2] 的处理性能。这种增强的处理能力有助于RS-4系列处理超出AE-4系列的任务，而以前这要求开发人员使用瑞萨的32位MCU。新型安全MCU能够以高速执行复杂的处理，可以更快地运行诸如Java Card™ *[3]或MULTOS*[4] 的多应用操作系统（OS），这对在单张智能卡上实现多种功能是非常必要的。此外，其低功耗设计使之适用于非接触操作。RS-4系列有助于开发人员使用一个16位MCU实现高性能和多功能的接触式或非接触式智能卡。

在安全方面，RS-4系列可以与AE-4系列一样执行金融领域要求的加密处理。此外，RS-4系列还增加了一个可支持更强大的AES（先进加密标准）加密及其他安全特性的协处理器。最终产品型号将为智能卡MCU提供最新版本的IT安全评估*[6] 共同准则规定的安全级别EAL5+*[5] 认证，这是目标市场所需的一种高级别安全认证。

<产品背景>

最近几年，为了对付伪造和数据偷窃行为，智能卡的应用正在不断增长，如包括传统信用卡和借记卡的信用卡和借记卡，以及包括护照、国家身份证、健康保险卡和驾驶执照等身份卡。与此同时，能运行Java Card™ 和MULTOS™ 等多种应用的通用操作系统的使用也在增加，而且用于身份验证等验证应用所需的处理也变得越来越复杂。这刺激了对具有改进的功能和性能的安全MCU产品的需求。由于其用户方便性和易于管理人员维护，非接触式智能卡越来越趋于普及。这种智能卡需要一个能够在有限的时间，使用很小功耗完成必要的处理工作的MCU，因此对更快的处理速度和更低功耗的需求也在增长。

瑞萨科技先前发布了AE-4系列高功能、高性能16位安全MCU，以及32位AE-5系列，后者的处理性能大约为AE-4系列的八倍。AE-4系列支持非接触操作，在非接触和双模（dual-way）智能卡的批量生产方面，给人留下了深刻印象的成功记录。新的RS-4系列是围绕RS-4 16位CPU内核开发的，可用来满足多功能和低功耗市场的需求。这个新开发的系列16位安全MCU结合了高性能和极其出色的价值。

- 更多 -

<产品细节>

新的RS-4系列的RS-4 CPU内核采用一种新开发的用于安全MCU的专有瑞萨架构。它有一个16位算术单元和一个16位内部总线。RS-4 CPU内核支持较早的代码级兼容的瑞萨AE-4 16位CPU内核的整个指令集。这意味着为AE-4系列开发的软件资源可以在RS-4系列上重新使用，从而减少了系统开发所需的时间和成本。与AE-4系列相比，RS-4系列旨在提供更高的性能、增强的安全性，以及改善的灵活性的更多的外设功能。RS-4系列的特性概括如下。

（1）相当于上一代产品五倍的处理性能，在运行先进的多应用操作系统时，可以使用16位MCU实现最快的运行

RS-4 16位CPU执行一个指令所需的最短时间为一个时钟周期。与此前的每条指令需要两个周期的AE-4 16位CPU相比，当在同样的时钟频率下工作时，RS-4系列的速度快了两倍。此外，RS-4不依赖于外部时钟，而是采用一个内部时钟振荡器作为其新的外设功能之一，以实现20 MHz的最高内部工作频率。这些改进的总体效果大约是AE-4系列处理性能的五倍*[2]。这种额外能力有助于RS-4系列更快地处理Java Card™ 或MULTOS™ 等多应用操作系统的复杂处理负载。如果不使用32位的AE-5系列，仅使用AE-4系列是无法实现上述功能的。最后，RS-4系列的低功耗设计使之适用于非接触式智能卡，而32位AE-5系列则不支持。RS-4系列可以用于接触式和非接触式智能卡。

（2）先进加密处理

新的RS-4系列的加密处理功能是由强大的模块化乘法加协处理器支持的，例如RSA加密和Triple DES（数据加密标准）协处理器，后者对以前的DES协处理器进行了改进。还有一个支持AES的新的协处理器，它是作为DES的继承者而获得关注的一个加密标准。RS-4系列可以高速处理各种类型的加密操作。

其他有利于提高安全性的外设功能包括：作为一种有效安全措施的高速产生随机数的新的伪随机程序发生器；可防止光攻击（light attack）的最新安全技术集成。因此，最终产品型号将为智能卡MCU提供IT安全评估共同准则规定的安全级别EAL5+认证，这是目标市场所需的一种高级别安全认证。

样品已作为一个开发工具开始交付，第一款RS-4系列逻辑芯片产品安装在仿真器*[7]上。这将有助于开发人员在2008年第二季度（4月至6月）样品交付开始之前就可以创建和评估软件。

开发工具的用户界面采用了高性能Embedded Workshop的标准瑞萨开发环境。它将有助于开发人员有效地使用一个接口创建和调试他们已经熟悉的程序。

- 更多 -

〈注释〉

注释： 1. 安全MCU：一种集成了加密功能并适用于智能卡等安全应用的MCU。

2. 在最高内部时钟频率和3.57 MHz的外部时钟频率下工作的性能，它是智能卡的标准操作环境。

3. Java和Java相关的商标和标识是美国Sun公司的商标。

4. MAOSCO（多应用操作系统）是MULTOS的商标。MAOSCO是一个制定、维护和管理MULTOS规范的联盟，具有MAOSCO Limited赋予的行政责任。

5. EAL5+：评估保证级别5+。EAL的“评估保证级别”是在IT安全评估共同准则中规定的，表示产品和系统的保证级别。其范围是从EAL1到EAL7的7个级别，以较大的数目表示更严格的保证级别。

6. IT安全评估（“CC”）共同准则是测量智能卡等IT产品安全保证的全球公认标准。CC 2.1版已被ISO/IEC标准15408采用。CC现已升级到3.1版，其中考虑了安全保证实践方面的最新进展。CC 3.1版已在欧洲、美国及日本的新的评估中采用。

7. 需要仿真器的开发人员必须签署一份保密协议。

＊ 其他提及的产品名称、公司名称或商标均为其各自所有者拥有。

〈典型应用〉

• 智能卡：ATM卡、信用卡、借记卡、电子货币卡、运输通行证卡、身份证，等等。

• 嵌入式设备：加密模块。

〈RS-4 系列规格〉

项目	RS-4 系列规格
CPU 内核	16 位 RS-4 CPU 内核
加密协处理器	• DES 加密协处理器 • AES 加密协处理器 • 模块化乘法协处理器
外设功能	• 内部时钟振荡器 • CRC 协处理器 • UART • 间隔定时器 • 其他
安全功能	• 检测电压、频率等反常的检测器 • 真伪随机数字发生器 • 检测定时器 • 片上存储器数据检查功能
接口	• 接触式：ISO 7816 • 非接触式：ISO 14443

-完-

媒体查询 – 瑞萨科技

中国:
瑞萨电子（上海）有限公司
郁聪
公共关系担当
业务企划部
电话：(8621)58771818*803
传真：(8621)68877858
Email:carrie.yu@renesas.com
http://www.cn.renesas.com

香港:
瑞萨香港有限公司
刘淑芬
市场推广经理
业务企划部
电话：(852) 2265 6611
传真：(852) 2375 6836
Email: silkie.lau@renesas.com
http://www.hk.renesas.com