

White Paper

The Right Kind of Microcontroller for Contactless Smart ICs

Joseph Pearson
Marketing Manager,
Government ID
RFID Systems
j-pearson2@ti.com

Zack Albus
Applications Manager
MSP430 Ultra-Low-Power Microcontrollers (MCU)
j-albus@ti.com

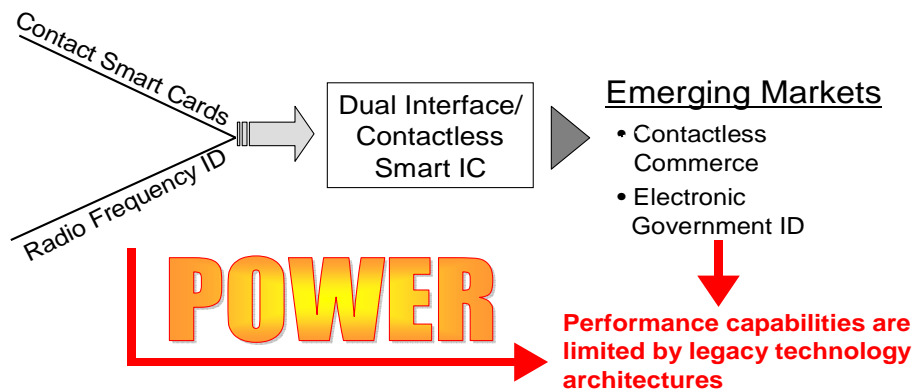
Introduction

The current generation of smart card ICs is anchored with older technology architectures that pose performance and transaction speed limitations especially for contactless applications. Legacy smart IC architectures are also restricted by high power usage and low data capacity which limit their scalability for future government identification (ID) applications. Today's commonly used 8-bit 8051 microcontroller (μ C) is at the mature phase of its life cycle. To better serve contactless and dual-interface contact applications, the smart IC microcontroller needs a low power design and a minimum 16-bit RISC (Reduced Instruction Set Computer) architecture. Next-generation contactless smart IC platforms, like the TI RF360, incorporate low power 16-bit RISC microcontrollers with contactless and security requirements integrated from the ground up to meet future application requirements in government ID and electronic payment markets.

Smart ICs and the need for low power

Legacy contact smart card IC technologies have been instrumental in the development of the contactless and dual-interface electronic government ID and payment card markets, and are still in use today. Contact smart card ICs were originally embedded into a plastic card the size of a credit card. They provided secure memory that could only be accessed by an authorized transaction and obtained power via a physical contact between the card reader and the smart card's 8-pin contact pad.

Convergence: Power Generated from the RF Interface



Graphic 1

In the early part of this decade, contactless and dual-interface smart ICs developed as a result of the convergence of contact smart card technology and radio frequency identification (RFID) technologies (Graphic 1). To create these contactless dual-interface smart ICs, most vendors modified their existing contact-based smart IC designs by adding RF analog front-end (AFE) circuitry. The AFE is both the power source for the smart IC and the communications interface to an RF reader using the ISO/IEC

14443 standard air interface protocol. As a result, today's contactless smart ICs are based on older technologies and architectures that were designed to operate with a direct power source and wired communications lines.

Passive power management was not an original design requirement; therefore, data processing efficiency in contactless applications and the RF link for power and communication are less than optimal. This affects transaction speed and performance which are important to production throughput of credentials and their level of operation in the field.

Government electronic identification credentials and contactless payment are two growing markets for smart IC platforms. And while the RF robustness and processing speed for reading and writing data have been adequate to establish these markets, low power efficiency limitations restrict future smart IC developments. Today, as security requirements increase, there are demands on memory size and transaction speed – especially critical for advanced government IDs – that cannot be adequately addressed with legacy technologies.

Memory and the Microcontroller

Two core legacy technologies that have limited the advancement of smart ICs are Electrically Erasable Programmable Read-Only Memory (EEPROM) and the 8-bit 8051 microcontroller. EEPROM is not power efficient compared with some newer types of memory like Ferroelectric Random Access Memory (FRAM). FRAM's fast access time, low power dissipation, small cell size, and efficient manufacturing process make it well-suited for next generation contactless smart ICs. (1) The advantages of FRAM are addressed on the TI web site: www.ti.com/govid. For a more in-depth discussion, view the TI white paper on FRAM at www.ti.com/rfid/govid/doccenter.shtml.

The 8051 μ C architecture originated decades ago and has become somewhat of a standard for microcontrollers in the 8-bit space. Numerous vendors have brought 8051-based platforms to market and it continues to be one of the most often used microcontroller architectures.

The key advantages of the 8051 μ C are its commonality and simplicity. Because of the longevity and popularity of 8051-based platforms, developers can leverage a deep wealth of existing software to minimize development time and financial investment. Another benefit of such an established architecture is the array of software development tools and equally broad number of 8051 μ C vendors.

One of the main disadvantages of 8051 microcontroller, however, is its accumulator-based central processing unit (CPU) design. The accumulator is used as a single location for temporary working data and memory operations, or operands. Instructions pass values to the accumulator where they are processed with additional instructions or data, modified and then passed onto their final destination, such as a port register or memory. With most instructions using the accumulator, this architecture often requires a number of instructions to be processed for a single operation to be completed. This affects code memory size, CPU processing bandwidth and time. In some cases, these instruction chains can also negatively impact real-time behavior where interrupt latency is critical.

Continuous optimization and improvements in performance are being made in the 8051-compatible space in the smart IC market. Newer 8051 derivatives typically offer additional peripherals that serve specific functions, such as extensions to enable faster CPU performance, code efficiency and support for larger memories. While this direction will surely keep the 8051 microcontroller alive for years to come, it does not address fundamental architecture limitations necessary for future scalability and transactional performance.

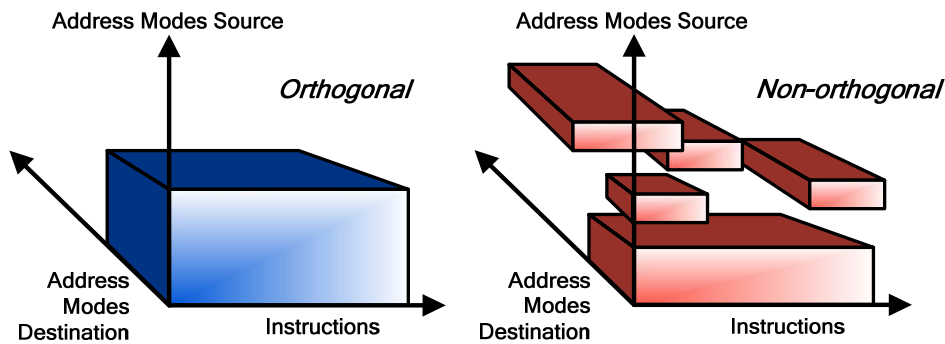
Efficient microcontroller architecture

To truly make next generation contactless smart ICs as efficient as possible, newer attributes of their architecture must be considered. A key design feature is a low power architecture which is needed to minimize the necessary energy converted from the reader's transmitted radio frequency signal for system operation. Further, contactless-enabled smart IC applications are powered only during operation via a contactless reader's externally transmitted energy. Therefore, the low power requirements fall directly into the microcontroller's active operation mode to execute a transaction and refer to low power consumption during CPU activity while performing program instruction execution.

Moving to a 16-bit microcontroller provides increased processing performance and data handling capability. In applications where data formats and calculations extend beyond 8-bits, such as in contactless smart IC applications, having a 16-bit CPU reduces the number of instructions needed per task, as well as the number of cycles required to process each task. Both of these improvements reduce the active 'operational' time of the processor and the energy consumption needed for a given task. However, it is not simply enough that the CPU core be extended beyond 8-bits. Incorporating a RISC architecture delivers significant efficiencies because it provides powerful instructions while using fewer of them. Compared to a typical 8-bit 8051 microcontroller, a 16-bit RISC microcontroller has fewer gates, which results in less switching, and consequently, lower power consumption when the CPU is active.

Architectural orthogonality is another key attribute to look for in an efficient microcontroller. As seen in Graphic 2, an orthogonal instruction set enables the use of each instruction across the IC memory with all addressing modes. A non-orthogonal approach can require additional instruction execution for a given task, potentially increasing execution time and code size. Orthogonal capability delivers powerful efficiency and flexibility in compiled code as well as CPU execution.

Orthogonal vs. Non-Orthogonal Instruction Set



Graphic 2

The advantages of moving from 8-bits to 16-bits beg the question: "Why not extend to a 32-bit architecture?" While it is reasonable to imagine such a microcontroller in low power applications, it is really a question of matching the right tool with the task. An argument can be made that the processing requirements for contactless smart ICs do not need 32-bit processing capability. Not only is such a microcontroller overkill, but 32-bit solutions are generally synonymous with high active power requirements for processing. Such microcontrollers are targeted for very highly intensive processing applications where active power is rarely a concern. In a smart IC application, 32-bit microcontrollers present a power budget requirement that complicates the contactless system as a whole and can compromise the overall application's performance.

Integrating a 16-bit processor that provides small code size and efficient low cycle count processing can be a key improvement to any system design. Doing so enables contactless smart ICs to be designed with less integrated memory that operate at low power without sacrificing CPU speed and performance.

Secure microcontroller architecture

A critical element in a contactless smart IC is security. And protecting the device from external threats begins early-on within the process of designing the microcontroller’s core architecture. While a microcontroller can be efficient and easy-to-use, it must include a range of security design elements that provide highest level of protection against undesired intruders.

Over the decades long history of smart ICs, there have been security tools and design best-practices developed to address the need for this strong security approach. These have been embodied in the stringent protection profile requirements of the international standard Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria) and cryptographic implementations by national standards, like Federal Information Processing Standards (FIPS) 140-2. Common Criteria establishes seven Evaluation Assurance Level (EAL) numerical ratings that describe the depth and rigor of an evaluation. The higher the EAL number, then the higher confidence that the system’s principal security features are reliably implemented. Including stringent protection profile attributes in the microcontroller design is paramount to having strong security within a smart IC and prevents attempts to compromise its data and integrity.

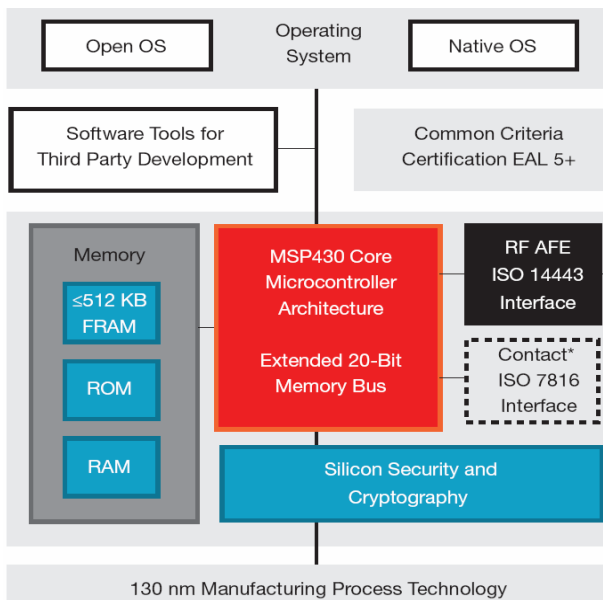
While the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have agreed to cooperate on the development of validated U.S. government Common Criteria protection profiles, other countries’ agencies, such as Germany’s Federal Office for Information Security known as BSI (Bundesamt für Sicherheit in der Informationstechnik) are generally accepted through certificates of mutual recognition.

Using an efficient, proven 16-bit microcontroller and having strong security is both possible and desirable. A smart ICs microcontroller should realize integrated strong security early in its design and be strictly enforced through the development of the final product.

RF360 Platform’s use of MSP430 microcontroller

Texas Instruments has taken a grounds-up approach to designing the next generation smart IC platform – the TI RF360. Graphic 3 depicts the Texas Instruments’ RF360 smart IC platform block diagram.

Texas Instruments’ RF360 Smart IC Platform

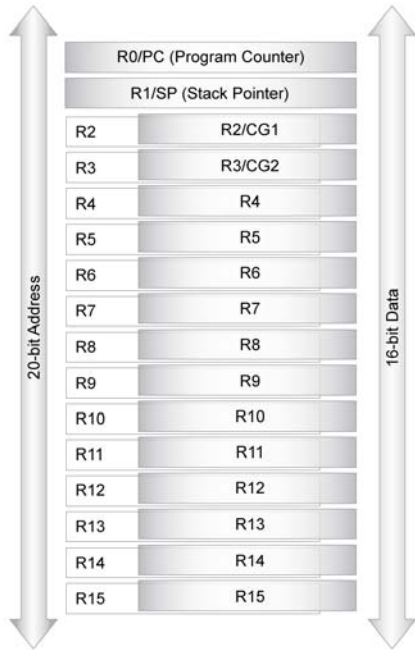


Graphic 3

In addition to other next generation technologies, such as FRAM, a 130nm CMOS RF Interface and a unified cryptographic engine; the heart of RF360 smart IC platform is the MSP430 16-bit, ultra-low power microcontroller core with a 20-bit extended bus memory. TI’s MSP430 core is a proven microcontroller designed into the RF360 IC architecture to deliver extremely efficient and fast processing capabilities. The MSP430 was originally developed in the mid 1990s for battery-powered metering and measurement applications. These applications required very low power consumption which resulted in long battery life and extended time between services.

Because off-the-shelf microcontrollers at the time were not ideal due to processing and power inefficiencies, the MSP430 was developed as a new kind of microprocessor core with ultra-low power consumption designed into every aspect of its architecture.

RF360's Extended 20-Bit Memory Bus



Since its inception, the MSP430 has evolved from one time programmable read-only memory (PROM) to in-system programmable flash which enables a wide array of applications and eases development. Newer peripherals ranging from 16-bit analog-to-digital converters to integrated operational amplifiers, segment-based liquid crystal display drivers and multi-channel direct memory access modules have all opened the door to more efficient and powerful system-on-chip application solutions.

Originally made up of sixteen, 16-bit registers, the CPU architecture has been extended to support 20-bit address reach, as seen in Graphic 4. This provides memory access beyond the 16-bit boundary without the inefficiency of paging found in many 16-bit microcontrollers.

With a total of twelve general purpose working registers (R4-R12), the MSP430 architecture eliminates the 8051's accumulator limitations, providing assembly developers and C-compiler vendors considerable flexibility. This fundamental architecture coupled with the fully orthogonal addressing modes/instruction set, achieves fewer instructions and lower execution times per task compared to 8051-based solutions.

Graphic 4

The MSP430's performance outpaces the 8051 in both code size and CPU cycle count as shown in Charts 1 and 2 across all test cases. (2)

MSP430 vs. 8051 – Code Size in bytes

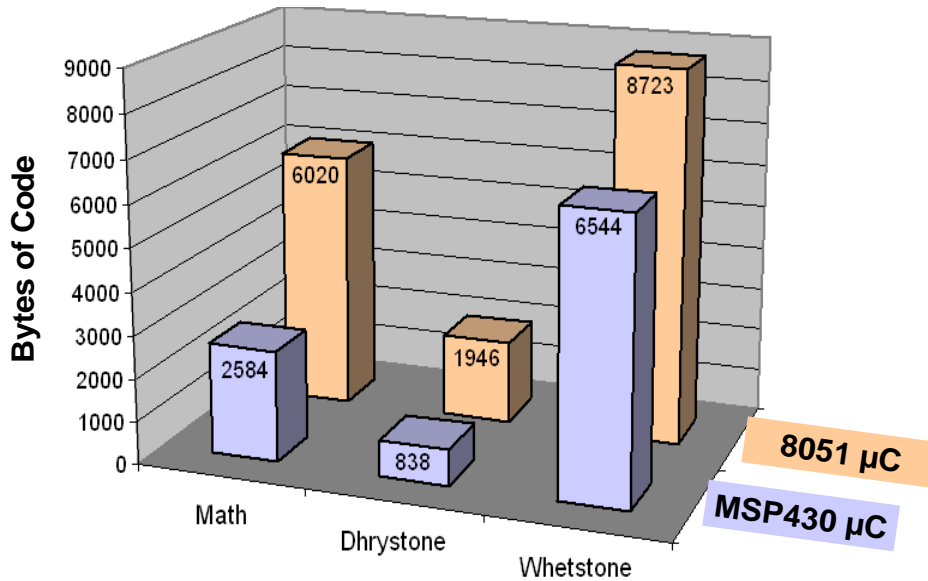


Chart 1

The data shows a marked increase in both code size and execution cycles for a given task on a standard 8051 compared to the MSP430. These tests range from 8 and 16-bit math operations and matrix handling to standard Dhrystone and Whetstone benchmarking. Across the three benchmarks, the MSP430 exhibited a 46% reduction in code size and 69% reduction in required processing cycles on average.

MSP430 vs. 8051 – Processing Time -- CPU clock cycles (in thousands)

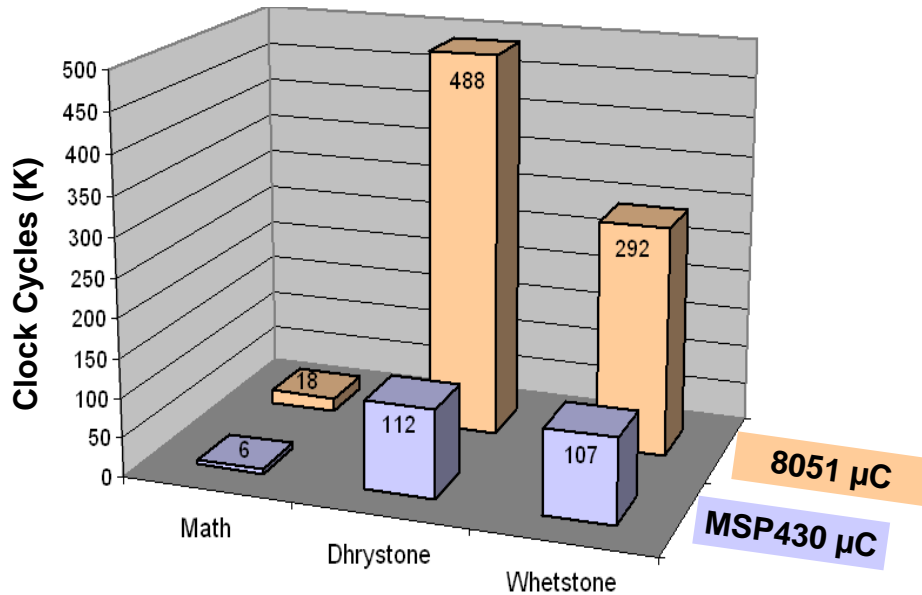


Chart 2

Non-standard versions of an 8051 can possibly show somewhat better performance results, but inherent limitations and capability thresholds inhibit their ability to come close to matching newer technologies such as the MSP430.

The 16-bit MSP430's architecture is ideal for applications such as contactless devices where ultra-low power is imperative. Its powerful code efficiency results in smaller integration requirements for system-on-chip designs and efficient processing performance – both critical to ultra-low active power consumption and transaction speeds. Further, due to the lower active power of the MSP430 core microcontroller unit (MCU), the RF360 exhibits both reduced electromagnetic system noise and potential interference when it is actively computing a transaction with an ISO/IEC 14443 standard contactless reader. The MSP430's integrated industry proven development and production tools, makes it is an ideal platform for many of today's low power embedded applications including the contactless smart IC design of TI's RF360 platform.

To ensure that strong security is a part of the RF360 platform, the MSP430 microcontroller has been integrated with all the necessary security features. TI has fully embraced the concepts behind Common Criteria and integrated it into the design of its RF360 smart IC platform. TÜV Informationstechnik GmbH (TÜViT), one the world's most respected and leading experts in smart card security and the Common Criteria process, is working with TI to verify its conformance to the process.

TI has selected the smart card IC Common Criteria Protection Profile BSI-PPP-0002 to define the minimum RF360 security requirements. TI intends to surpass the basic EAL4+ BBSI—PPP-0002 requirements to achieve EAL5+ certification. In addition, the RF360 supports FIPS-140-2 compliant symmetric (DES & AES) and asymmetric (RSA & Elliptic Curve) cryptographic algorithms with fast hardware co-processors.

Conclusion

Electronic government ID applications are demanding more speed and functionality from contactless smart ICs. As security threats escalate, ID volumes dramatically increase, governments begin to integrate extended biometric functionality and multiple applications, contactless smart ICs need to incorporate a multitude of new capabilities. These include higher security, faster processing and production throughput and quicker transactions that positively impact the user experience.

To achieve these faster transaction speeds, while maintaining necessary strong security, the right kind of microcontroller for contactless smart ICs is a 16-bit RISC microcontroller core designed with an orthogonal instruction set and stringent security attributes and countermeasures. Compared to a typical 8-bit 8051 found in many older smart IC platforms, a 16-bit RISC microcontroller uses less code and lower power to process data. These attributes, along with other next-generation technologies like FRAM non-volatile memory, enable smart IC platforms, such as the TI RF360, to be best suited to meet requirements in government ID and electronic payment applications.

Source 1: "The Advantages of FRAM-Based Smart ICs for Next Generation Government Electronic IDs"; Joseph Pearson and Dr. Ted Moise; Texas Instruments, Inc.; September 27, 2007

Source 2: "MSP430 Competitive Benchmarking"; Greg Morton and Kripasagar Venkat; Texas Instruments, Inc.; SLAA205B, July 2006

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

All trademarks are the property of their respective owners.