

Secure solutions for high-performance 32-bit processing

ARM's SecurCore family provides unique, 32-bit solutions for smart card and secure IC development — offering system designers privileged access to ARM® processor cores to create fast, secure e-commerce, banking, networking, mobile multimedia, identification and mass transit solutions.

The ARM SecurCore family currently comprises the SC100 core, the SC110 core, the SC200 core and the SC210 core. The SecurCore family provides an ideal migration from 8/16-bit to 32-bit smart card and secure applications, and delivers a comprehensive range of secure functionality.

ARM SecurCore processors offer all the benefits of the industry's leading high-performance, low-power 32-bit RISC microprocessing technology, with significant design enhancements that make the ARM approach ideal for secure applications.

The SecurCore Family Benefits

The ARM SecurCore family is based on proven ARM 32-bit RISC technology and offers some of the most advanced security features for smart card and secure IC applications.

- Synthesizable design to allow custom development for added security
- Security features to resist tampering and reverse engineering
- Randomized layout based on customer design specifications
- Debug and test methodology purpose-designed for secure systems
- One-way design information flow to ensure secure development process
- ARM Memory Protection Unit for secure isolation between OS and applications
- Standard development tools to reduce time-to-market and costs
- Thumb® code density (typically a 30% reduction in code size)
- Fully code-compatible with established ARM7™ and ARM9™ processor families
- OS support for Java Card and MULTOS
- RTOS capability for advanced networking security applications
- Coprocessor support
- High-end cryptographic accelerator (optional)

The SecurCore SC200 and SC210 cores offer these additional features:

- Enhanced core security including extended MPU
- ARM Jazelle™ technology for optimized Java Card acceleration

Why ARM Technology is Ideal for Secure Applications

The ARM SecurCore family provides a secure processor design and anti-counterfeiting methodology that is unique to ARM and which helps resist invasion and physical tampering at the hardware and software levels — whether through applying power or timing analysis, directly probing the chip surface or reverse engineering the layout.

jazelle™

ARM Jazelle technology is an extension to the world's leading 32-bit embedded RISC architecture, enabling ARM processors to execute Java bytecode directly in hardware and delivering unparalleled Java performance on the ARM architecture.

Jazelle technology can improve performance up to 8x compared to a software Java Virtual Machine (JVM) (embedded CaffeineMark3.0).

Jazelle technology also ensures compatibility with existing operating systems, interrupt handlers and exception code. Up to four stack elements are maintained in ARM registers to reduce memory access to a minimum; this is an important contributor to the excellent performance of the processor when executing a Java application. Stack spill and overflow is handled by the hardware.

reduced. This reduction can result in the Jazelle technology logic being accommodated with a net reduction in silicon area.

Power and Energy Saving

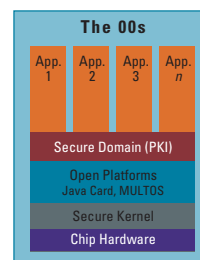
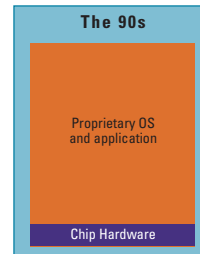
Direct execution of bytecodes reduces the memory activity levels in the system by approximately 40%. This reduction, together with the efficiency gains from Jazelle technology, results in the energy consumption for a typical Java Card application being reduced by up to 80%, enabling the running of Java Card on a contactless smart card to become a practical reality.

Performance Without Penalty

ARM processor technology has several unique advantages over traditional microprocessor solutions in terms of optimum performance, small die size, and extremely low power consumption. For example the ARM architecture is optimized to run interpreted languages efficiently. It is therefore already an ideal platform for Java Card or MULTOS. Thumb® code compression allows the ARM core to compete very effectively on natively compiled code. The Jazelle™ Java hardware accelerator technology and Thumb code provide real performance enhancing capability in highly compact systems. High performance multipliers allow good native cryptographic performance.

ARM SecurCore SC100 Cores

The SC100 core and the SC110 core, incorporating a cryptographic accelerator, provide a low cost route to migrate smart card designs to the 32-bit ARM platform. The SC100 family supports the ARM and Thumb instruction sets, integrated memory protection unit and many specific security features.



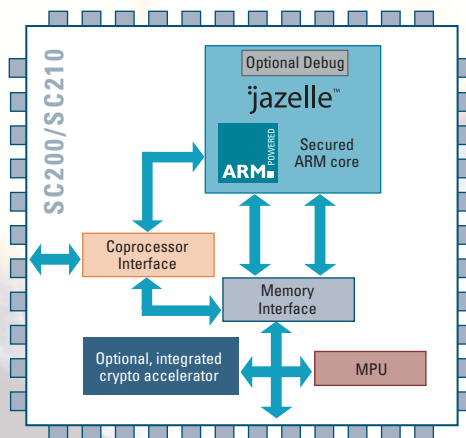
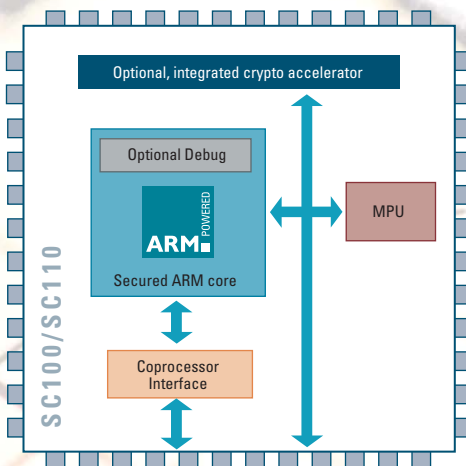
THE SMART CARD EVOLUTION

SecurCore SC200 Jazelle™ Accelerated Cores

ARM's SC200 and SC210 cores integrate an optimized implementation of Jazelle technology for Java Card, offering smart card and secure IC developers important benefits:

Reduced Memory Footprint

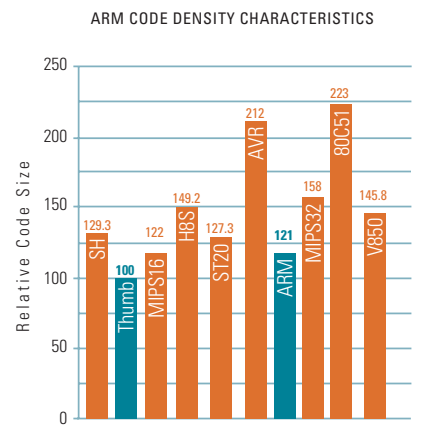
Direct execution of the majority of bytecodes by the Jazelle technology accelerator enables the size of the byte code interpreter to be significantly



Thumb® Instruction Set

ARM technology supports a standard, 32-bit instruction set, and a compressed instruction set called ARM Thumb code. Thumb instructions are a subset of the most commonly used 32-bit ARM instructions that have been compressed into 16-bit opcodes. On execution, these 16-bit instructions are decompressed to 32-bit ARM instructions in real time without performance loss.

Designers can use both 16-bit Thumb and 32-bit ARM instructions sets and therefore have complete flexibility to compile for maximum performance or minimum code size as their applications require. Typical memory savings of 35-40% on native smart card code can be achieved.



Higher Performance

Jazelle provides the highest performance of any Java Card solution available. Close integration into the ARM core provides exactly the right tradeoff of power and area while offering optimum performance in a smart card.

Ease of System Integration

Jazelle technology is fully integrated into the industry-leading ARM RISC architecture and is

| ARM SecurCore Family Characteristics | | | | | |
|--------------------------------------|---------------------------------|-----------|----------------|------|---------------------------------|
| Product | Die Size (mm2) / Gate Count (K) | | Power (mW/MHz) | | Speed (MHz) 0.18µ worst case |
| | 0.18µ | 0.25µ | 1.8V | 2.5V | |
| SC100 | 0.6 / 33 | 1.3 / 33 | 0.30 | 0.63 | >66 |
| SC110 | 1.42 / 78 | 2.84 / 78 | 0.35 | 0.74 | >66 |
| SC200 | 1.0 / 55 | 2.0 / 55 | 0.40 | 0.84 | >100 |
| SC210 | 1.8 / 100 | 3.6 / 100 | 0.40 | 0.84 | >100 |

Silicon area for only 3 utilized layers of metal

completely compatible with the ARM interrupt and exception model — giving easy design and integration with existing secure operating systems and applications. A single processor can be used for both Java Card and existing OS and applications in the development of software for smart cards and secure devices.

| SecurCore RSA Crypto Performance at 20MHz | | |
|--|---|-------------------|
| Core | Signature authentication and encryption | |
| | 1024-bit | 2048-bit |
| SC110 / SC210 | <1.5ms | <12ms |
| SC100 | 33ms | 128ms |
| SC200 | 21ms | 80ms |
| Signature generation and decryption | | |
| SC110 (with CRT) SC210 (with CRT) | 25ms | 300ms |
| SC110 (without CRT) SC210 (without CRT) | 95ms | 1500ms |
| SC100 (with CRT) SC200 (with CRT) | 525ms 330ms | 3690ms 2215ms |
| SC100 (without CRT) SC200 (without CRT) | 1715ms 980ms | 13370ms 7580ms |

CRT: Chinese Remainder Theorem

Integrated Crypto Solutions

Easy incorporation of proprietary cryptographic solutions

The ARM SecurCore family also permits ARM partners to customize the core by adding a range of security features known only to the card issuer/developer.

ARM has number of solutions for implementing cryptography in the core, the use of which are determined by the target application and licensee technology.

All SecurCore processors incorporate a standardized coprocessor interface, enabling

customer-designed cryptographic processing extensions to be added to the ARM instruction set. This is particularly relevant in emerging or specialist markets, where proprietary or secret cryptographic algorithms must be easily integrated with the core. The coprocessor instruction space is reserved in the ARM architecture, and is extensively supported by ARM and third party tools.

Best-in-Class Integrated Crypto Processing

In addition to the coprocessor interface, ARM has also integrated a leading-edge cryptographic engine, the EIP-25™ from Safenet, into the SC100

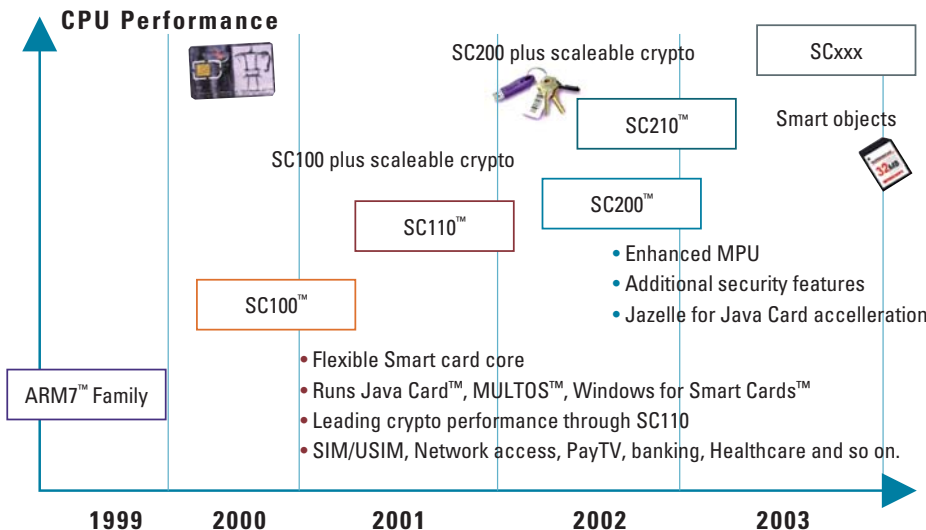
and SC200 cores to produce the SC110 and SC210 cores. This cryptographic engine gives the SecurCore solutions best-in-class performance with low power.

The configurable cryptographic engine enables the implementer to choose the trade-off between performance and area according to the application. The architecture implemented has a number of innovative features including scaleable parallel processing elements and also implements advanced features to resist power and timing attacks.



Open Interface for Third Party Cryptography

In addition to the integration of SafeNet's EIP-25 cryptographic engine into the SecurCore roadmap, ARM also provides SecurCore licensees the flexibility to integrate either their own cryptographic solution or third party cryptographic technology.



A Complete Solution

ARM provides developers with intellectual property (IP) in the form of processor core designs, cache and SoC designs, application-specific standard products (ASSPs), related software and development tools — everything you need to create an innovative product design based on industry-standard components that are ‘next generation’ compatible.

ARM Design Tools for SecurCore

ARM technology offers developers a range of tools that provide a seamless development route from emulation software through board-level integration to trace and debugging.

ARM’s advanced debug technology provides optimum flexibility in the construction of development silicon and system for ARM core-based smart cards and secure SoC. The debug facilities are combined with a methodology which ensures that, once the smart card or secure IC design is proven in development, these features are removed from production silicon to prevent attempts at reverse engineering for added security.

For security purpose, the SecurCore Tools Enabling Kit is an add-on of plug-ins to the Real View tool chain that allows the simulation and target debug of SecurCore processors. This kit is available free of charge to the users of the ARM Real View tools who have a current maintenance contract with ARM. The availability of this kit is subject to the acceptance of an end-user license agreement that protects the information it contains.

RealView™ Development Solution

The RealView Development Solution provides best-in-class tools for system development, debug and prototyping. RealView reduces risk, improves

productivity and quality of results for all systems based on the ARM Architecture.

RealView Debug

The ARM RealView Debugger is a leading component of ARM’s new RealView Development Solution. It delivers multi-core mixed architecture debugging and OS aware debugging of applications for all ARM core-based devices.

The RealView Debugger complements ARM’s existing tools solutions, ARM Developer Suite™ (ADS), Multi-ICE® and MultiTrace™, as well as providing performance improvements when used with the new RealView ICE and RealView Trace module.

RealView ICE

High-speed code download and fast stepping speeds are essential requirements of the debug process.

RealView ICE delivers high performance in-circuit emulation through a standard JTAG TAP port at data rates of 600kBytes/s. It is capable of supporting JTAG clock frequencies of up to 50 MHz, providing even higher throughput.

This in conjunction with support for all current ARM cores and the ability to add additional modules for extra functionality such as Trace capture makes RealView ICE an essential tool in the ARM system debug environment.

RealView Compilation Tools

The RealView Compilation Tools provide the full set of software components required to build C and C++ applications targeting the 32-bit ARM and 16-bit Thumb instruction sets.

The C and C++ compilers provide industry leading code density and performance optimizations for all members of the ARM processor family.



RealView Compilation Tools include: Optimizing ANSI C Compiler, Optimizing Embedded C++ Compiler (EC++) , Linker, Assembler, Image Conversion Tool, ARM Object file Librarian/Archiver, C Libraries, RogueWave C++ Libraries

RealView Platforms

The ARM Integrator® family leverages ARM’s unique experience in test chip technology to provide a range of flexible, high-performance development platforms that meet the needs of today’s system-on-chip developers.

Integrator platforms enable the integration of software and hardware IP such as ARM cores, ARM PrimeCell peripherals and their associated drivers, operating systems and application software.

Integrator reduces development times and increases levels of confidence in the final silicon by allowing early prototyping of an environment similar to the final system using both programmable and standard components.

ARM e-Commerce Design Center

ARM has established an e-Commerce design center, based in Sophia-Antipolis, France.

Using the skills of smart card developers and e-Commerce specialists combined with ARM’s own engineering expertise, the center is uniquely placed to develop card-based secure systems technology within a purpose-built, security-controlled environment.

The group skills are:

- Several years of experience in secure chip design
- Secure environment implemented
- Dedicated resources
- Expert in secure core design
- Training and support services for ARM SecurCore family cores

ARM, ARM Powered, StrongARM, Thumb, Multi-ICE, Integrator, PrimeCell and ARM7TDMI are registered trademarks of ARM Limited. ARM7TDMI-S, ARM7EJ-S, ARM720T, ARM740T, ARM9TDMI, ARM920T, ARM922T, ARM940T, ARM9E, ARM926EJ-S, ARM946E-S, ARM966E-S, ARM1020E, ARM1022E, ARM1026EJ-S, ARM11, EmbeddedICE, EmbeddedICE-RT, AMBA, MultiTrace, ModelGen, ARM Developer Suite, RealView, ETM, ETM7, ETM8, ETM10, Embedded Trace Macrocell, Jazelle, PrimeXsys, MOVE and JTEK are trademarks of ARM Limited. Java is a trademark of Sun Microsystems, Inc., XScale is a trademark of Intel Corporation. All other brand names or product names are the property of their respective holders. ‘ARM’ is used to represent ARM holdings plc (LSE: ARM and NASDAQ: ARMYH), its operating company ARM Limited and the regional subsidiaries ARM, INC.; ARM KK; ARM Korea Ltd. Neither the whole nor any part of the information contained in, or the product described in, this document may be adapted or reproduced in any material form except with the prior written permission of the copyright holder. The product described in this document is subject to continuous developments and improvements. All particulars of the product and its use contained in this document are given by ARM in good faith. All warranties implied or expressed, including but not limited to implied warranties of satisfactory quality or fitness for purpose are excluded. This document is intended only to provide information to the reader about the product. To the extent permitted by local laws ARM shall not be liable for any loss or damage arising from the use of any information in this document or any error or omission in such information.

