

# Secure Megabytes on your Smart Card

## Presented by

Ian Duthie  
Marketing Manager,  
Smart Card ICs  
Atmel Corporation

[Iduthie@atmel.com](mailto:Iduthie@atmel.com)

Barry Hochfield  
Technical Director  
Ecebs Ltd

[BarryHochfield@ecebs.com](mailto:BarryHochfield@ecebs.com)

25-Nov-05

Card Forum International

January 2004

## Introduction

The typical smart card today has anything from 2K bytes of EEPROM up to around 72K bytes of EEPROM, with products in development offering 100K to 300K bytes. To jump to Megabytes of secure data storage may seem a little unrealistic to many people looking at traditional smart card applications for a product available in the short term. However, Ecebs, an advanced technology company, specialising in rapid smart card solution development, has already brought to market just such a product. This paper describes the development and introduction of a secure data storage product having 4 Megabytes of Flash data memory with a high security, high performance RISC microcontroller, packaged in a standard ISO 7810 smart card module format. This product is qualified and in production today. Within twelve months this capacity can be increased to 8 and even 16 Megabytes.

The driver and technology development of such a product family now follows.

## The Origin

In 2001, Ecebs was awarded the development of the ITSO Secure Application module (ISAM) for the UK transport-ticketing organisation, known as ITSO (Integrated Transport Smartcard Organisation). The ISAM enables the use of interoperable smart cards for transport and other ticketing via a common interoperable specification at both the card and application level. Central and key to the overall system is the ISAM, which allows easy financial reconciliation of all the different ticketing products across different schemes in the UK. However, storage of all the transactions taking place at each terminal as well as storage of all the different product and scheme keys, required a solution having a large data capacity as well as having to be as secure as a standard smart card. The solution lay in the development of the High Capacity Secure Microcontroller chip set.

## The High Capacity Secure Microcontroller

This 2 chip solution comprises

- ◆ Greater than 80x the capacity of typical secure microcontroller with 32, 64 or 128Mega-bit of re-loadable fully secure memory
- ◆ Atmel's high security, high performance secureAVR™ microcontroller (8/16-bit RISC core)
- ◆ Powerful cryptoprocessing capability with DES/TDES and RSA for fast data encryption/decryption
- ◆ FLASH flexibility for program memory
- ◆ High security with Common Criteria certification to EAL4+
- ◆ Flexibility and extensibility for development support

The high-density storage capacity is achieved by integrating Atmel's Flash Memory with its secure microcontroller, and housing the components in a standard SIM format package.

The design concept for both software and hardware was that of Ecebs, however, for such a product to be successful it was necessary to develop a close partnership with both a provider of secure microcontrollers and an advanced technology module manufacturer. Since Atmel was already a leading provider of secure microcontrollers and renown for its Flash technology, it was a natural choice. Sagem, as a manufacturer of smart card systems, was able to offer specialist support in the development of a dedicated module, and thus provide the packaging expertise to meet the stringent requirements of this product, i.e. to still be able to comply with an ISO 710 SIM form factor and mechanical constraints.

## The First Product

### The AT90SC3232CS-F32M High Capacity Secure Microcontroller

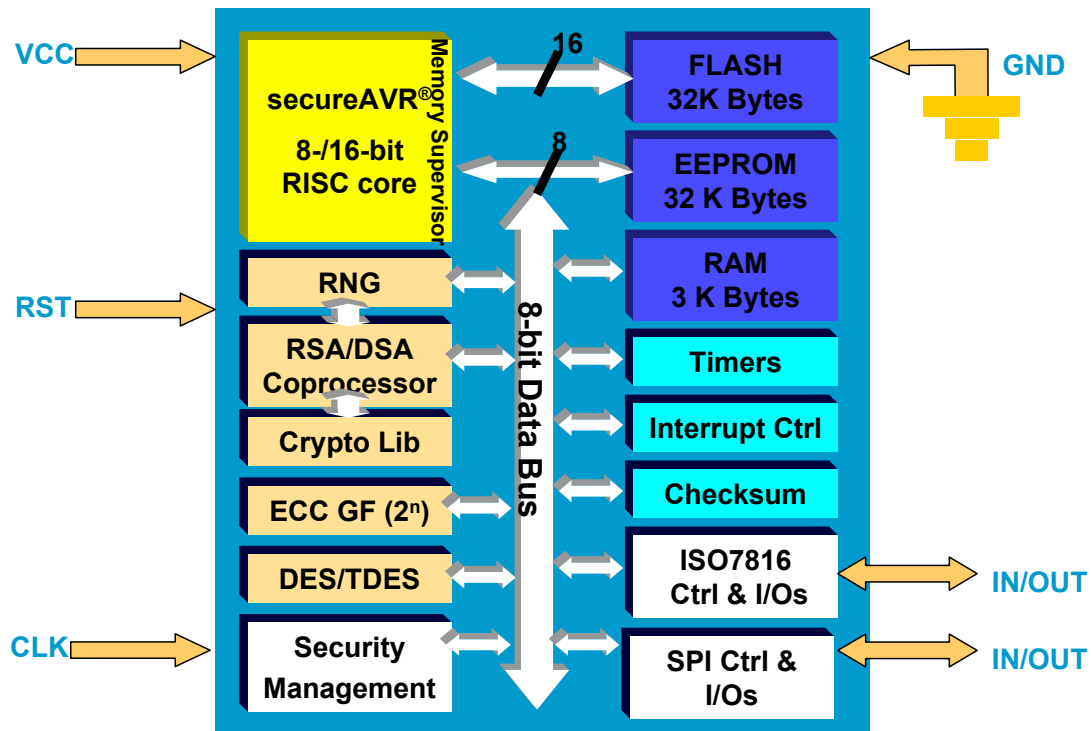


Figure 1. AT90SC3232CS Architecture

The silicon hardware is based on Atmel's secureAVR™ 8/16-bit RISC microcontroller family, utilising the full features of the AT90SC3232CS microcontroller. Its architecture is shown in Figure 1. It comprises 32K bytes of Flash Program memory as well as 32K of EEPROM for data memory and 3K RAM, which is sufficient to support its full crypto processing capability derived from the core offering up to 20MHz computing power along with its two co-processors. One coprocessor being a 16-bit RISC processor for Public key algorithms such as 2048-bit RSA, DSA, SHA-1 hash, etc, the other a fast DES/Triple DES processor capable computing a DES in 16 cycles  $\Rightarrow$  0.8 $\mu$ s. In addition there is a GF(2<sup>n</sup>) accelerator for Elliptic Curve Cryptography (ECC), as well as software toolbox and libraries.

From the security standpoint, it features the secureAVR environmental protection system, including an efficient MMU for multi-application and the hardware DES provides exceptional power analysis resistance. The device is the first Flash based microcontroller to achieve Common Criteria certification to EAL4+ (augmentation to AVA\_VLA4).

The implementation of Flash rather than ROM for program memory makes the device very versatile for a wide range of security applications, allowing fast development cycle times and early pre-production. Atmel recognised the potential of interfacing to external memory and added in addition to the standard ISO 7816 port, a serial peripheral interface (SPI) port, which Ecebs has capitalised on by integrating the microcontroller with Atmel's 32M-bit Flash memory, the AT45DB321B. Both devices are embedded with additional circuitry in Sagem's custom designed module and with patented security software from Ecebs, all data between the microcontroller and the Flash memory is encrypted, preventing any would be hackers from performing "man-in-the-middle" attacks between the two devices. This high capacity secure IC architecture is illustrated in Figure 2. with examples of the module shown in Figures 3 and 4.

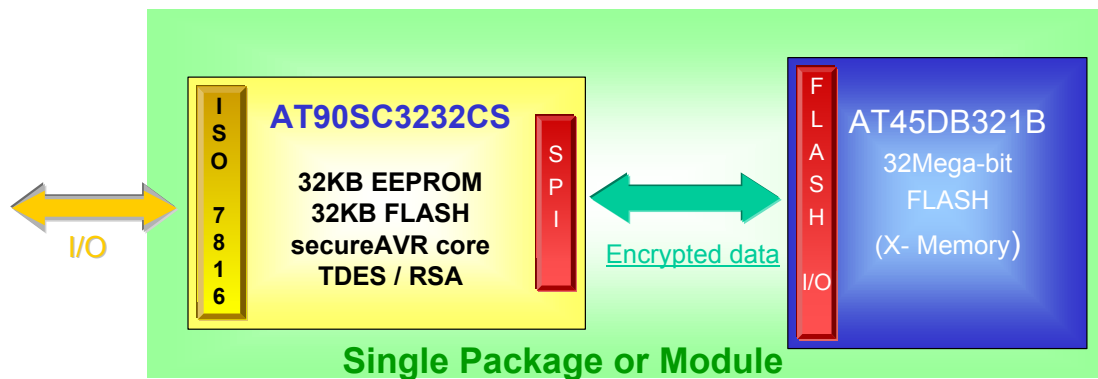


Figure 2. High Capacity Secure IC Architecture

### From Chip Set to Card

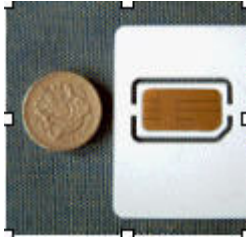
Putting it simply, to turn the Atmel AT90SC3232CS-32M chip set into a true High Capacity SmartCard, Ecebs had to:

- ◆ Design additional circuitry to allow the AT45DB321B to operate over the full smartcard voltage range of 2.7V to 5.5V,
- ◆ Design the substrate for the module (in conjunction with and to suit Sagem's production processes), and, most importantly,
- ◆ Develop a software library that both integrated the Data flash into the operating system running in the AT90SC3232CS and fully secured the data in the external flash memory.

To consider the product a true 4 Megabyte smartcard, one had to ensure that the data in the external memory is 'as secure as if it was inside the smartcard device's own internal EEPROM.' At first thought this may seem obvious; simply encrypting all the data in the external flash one would achieve this goal. However, this is not so for the following reasons. The key or keys used to encrypt the data stored in the external Flash must be treated with a level of security such that the data in the external flash can be considered as secure as the data in the internal EEPROM. Therefore these keys must never be read or even exist outside of the AT90SC3232CS's internal EEPROM. To achieve this, the AT90SC3232CS's Random Number Generator was employed to generate a triple DES key pair unique to each chip set. This same software only accesses these keys as part of the encryption/decryption process between the AT90SC3232CS and the external Flash memory (X-Mem).

But encryption of the data is not in itself sufficient to meet the 'as secure as inside' claim. One must also protect against 'replay attacks'. A replay attack is a very potent attack because the attacker does not need to decrypt data at all. If the system is designed in a naive fashion such that data with inherent 'value' can be identified when being moved between the X-Mem and the AT90SC3232CS through the SPI, then that, still encrypted, data can be 'siphoned off' and replayed at the appropriate moment to the SPI thus fooling the system into thinking there is value present that had already been spent.

Simply adding unique session keys to each page in the external flash, while appearing to solve this problem only serves to clog up the internal EEPROM of the AT90SC3232CS with hundreds of keys, not a practical solution. However, Ecebs has solved this problem, which is the subject of a pending patent. It is this software that turns the Atmel chip set into the High Capacity Card (HCC™).



**Figure 3. The HCC ISO compliant module**

## Product Options

Ecebs have exclusive rights to market the High Capacity Card (HCC™) and can provide three configurations to suit all customers. For example, Option One: if the customer wishes to develop his/her own Operating System running in the AT90SC3232CS, Ecebs can supply the High Capacity Card –Secure Link Library (HCC-SLL™). The HCC-SLL™ consists of a programmer's guide and a Library Module that extends the standard Atmel Software Development Kit for their secureAVR™ based smartcard micro-controllers. As this library makes use of both the AT90SC3232CS's RNG and DES/Triple DES processor in a Power Analysis Attack resistant manner, these lower level API's are also available to the developer to save them time and effort re-inventing them. In this way the HCC-SLL also provides the makings of a Hardware Abstraction Layer to speed up subsequent development.

Option Two: is where Ecebs can make available 'Mfos™' a complete Card Operating System (COS) that provides all the other aspects of a Hardware Abstraction Layer with other COS services for enablement and personalisation. This option enables further custom application development quickly and securely.

For Option Three: Ecebs can provide a turn-key solution of application and operating system, similar, for example, in nature to the work done for the ITSO SAM, where a full ISO 7816-4 secure file system and several bespoke APDU's with application specific logic are developed allowing the solution to be deployed in record time. The HCC™ also supports the revolutionary application, management and security solution, 'Multefile™' which enables simultaneous generation of, card and terminal applications from one GUI tool, obviating the need for code writing completely.



**Figure 4: The HCC as the ITSO SAM.**

## Conclusion

A fully 7816 compliant smartcard with storage capacity in the order of Megabytes is now a reality and is being delivered to enable market growing applications such as interoperable ticketing. What other applications for these devices is only now being understood, but as GSM has driven the memory size requirements of the smartcard ahead of other market sectors, this is clearly a candidate application for the HCC. Other potential application areas include Military records, Medical health records, Secure inventory management, portable HSM/Key repository, as well as other high density secure data storage.

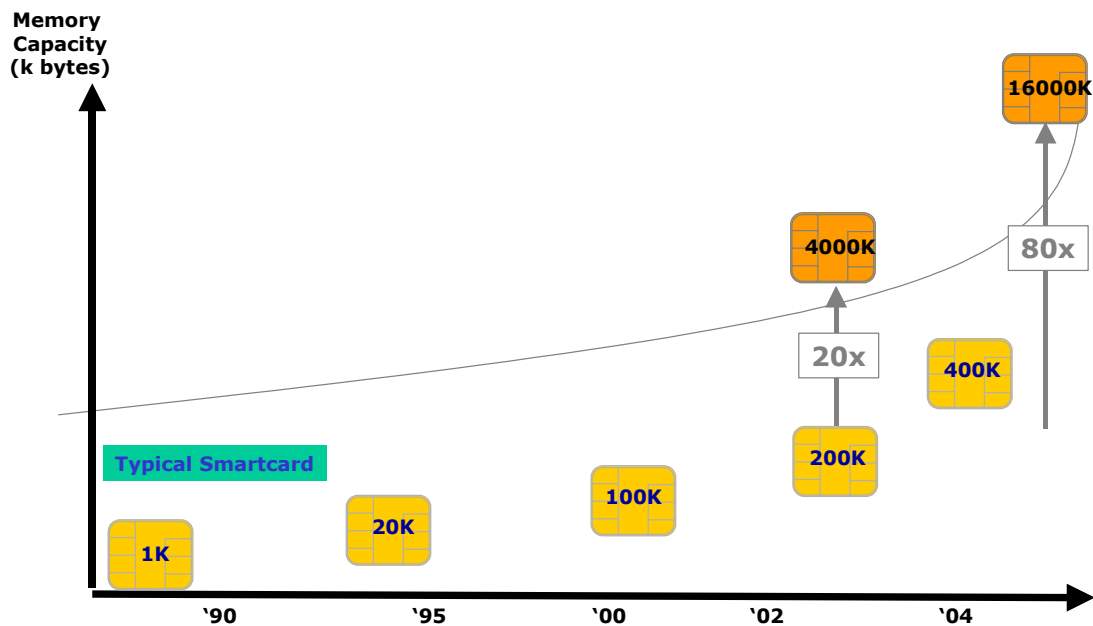


Figure 5. High Capacity Secure ICs Evolution

With technology shrinks, it is an easy upgrade to replace, for example, Atmel's 32M-bit Flash with its new 128M-bit Flash. A high performance device is also planned with Atmel's 32-bit Secure Microcontroller AT91SC25672RC, as an alternative to the AT90SC3232CS.

## Biographies



### Barry Hochfield

Barry is co-founder and Technical Director of Ecebs Ltd. He has over twenty-four years' experience in IT and computing including marketing, and general management with nine years focussed on smartcard technology. He has held senior positions at Apple Computer, Motorola Semiconductors, Mondex International and Keycorp. He was responsible for developing the specifications for the smartcard industry standard multi-application operating system MULTOS 4.0, and holds several patents in smartcards and other IT fields.



### Ian Duthie

Mr. Ian Duthie has an MSc in Computing for Commerce and Industry, is a Chartered Engineer and a Member of the Institute of Electrical Engineers. Educated in the UK he is currently employed as a worldwide Marketing Manager for Atmel's Smart Card ICs Division, based at East Kilbride, Scotland, UK.

Mr. Duthie has seen the Smart Card market grow from its embryonic days in the 1970's while at Motorola when its chip design team developed the first microprocessor Smart Card on behalf of Bull-CP8. He joined the Smart Card marketing team in 1992 and has presented the silicon vendor's viewpoint on Markets, Technology and Security, in Smart Card journals and at leading international Smart Card conferences in Africa, Asia, Europe and the US. He is currently employed by Atmel since its acquisition of the Smart Card chip division of Motorola in April 1999.