

The Advantages of FRAM-Based Smart ICs for Next Generation Government Electronic IDs

By Joseph Pearson and Dr. Ted Moise
Texas Instruments, Inc.
September 27, 2007

Executive Summary

Electronic versions of passports and other government-issued identification documents use an Integrated Circuit (IC) or chip to establish a digital link between the holder and personal biometric information, such as a digitized photo, fingerprint or iris image. Designed to enhance border, physical and IT security, electronic chips ensure that the person holding a passport or government document is the one to whom it was legitimately issued.

The next generation ICs will employ an advanced embedded memory technology, called FRAM (Ferroelectric Random Access Memory), which considerably improves the speed and reliability of future smart, secure e-passports and government ID documents. More than 50 countries have electronic passport (e-passport) programs, and many countries are also putting in place more secure forms of electronic citizen, visitor and government employee identification. As the volume of document issuance increases and new security threats occur, there is an increased need for industry-standard, next-generation contactless smart IC solutions that securely store, process and communicate data. These new smart ICs will have increased writing speeds to produce and process documents faster and more efficiently, as well as enhanced memory for future security requirements.

When FRAM is manufactured at the 130 nanometer semiconductor process node, and embedded in a smart IC, it surpasses the limitations of current Electrically Erasable Programmable Read-Only Memory (EEPROM) and other memory technologies used in government ID applications. The imminent introduction of this innovative memory technology for smart ICs signals a shift in performance in smart card applications deployed in government electronic ID documents.

This paper details the advantages of embedded FRAM memory for smart ICs in contrast to the traditional memory technologies used in many e-passport and government ID programs today.

Performance and Functionality Gaps in Legacy IC Technologies

While some government-issued electronic ID documents have employed traditional secure contact smart card technology, many new applications use dual interface or contactless smart ICs developed as a result of the convergence of contact smart card technology and Radio Frequency Identification (RFID) technologies. As the names imply, contact smart cards work by obtaining processing power and communication via physical contact between the card reader and the smart card's 8-pin contact pad, while contactless smart cards are powered and communicate by means of a Radio Frequency (RF) signal. To create the existing generation of secure e-passports, most smart IC 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, such as those used in e-passports, are based on older technology architectures where neither passive power management nor RF communications speed were original design requirements.

While legacy smart IC architectures enabled the creation of first-generation government electronic ID applications, writing and reading data on the chip is slow, and the RF link for power and communication is less than optimal. This negatively affects throughput and quality in credential production and the level of read performance in the field. New contactless RF-enabled chip technologies developed specifically for e-passport and other electronic government ID programs have several advantages. They will deploy the latest microcontroller and RF advances while using ultra low power, fast memory and high levels of security. The next generation of smart ICs will have faster data write and transaction read times to improve document issuance and personalization times, meet new security requirements and enable new applications in future iterations of government IDs.

EEPROM and Flash Memory: Widely Used, but Limited Capabilities

The performance and capabilities of current government-issued electronic identification documents are limited by the type of memory technology used on the IC. The primary memory technologies used on these chips are Electrically Erasable Programmable Read-Only Memory (EEPROM) or Flash. Flash is a variation of EEPROM that can be erased and reprogrammed in units of memory called blocks rather than bytes.

Like FRAM, both EEPROM and Flash are non-volatile memory technologies, which mean they don't lose their data contents when power is removed. Unlike FRAM, EEPROM and Flash employ a floating gate charge storage design approach that operates by bringing electrons onto a polysilicon floating gate isolated by an oxide insulator. To reliably produce and store the data, a thick oxide (of 80-100 Å) is required, necessitating a high voltage of 10-14 volts to embed the electrical charge. To create the high voltage on the IC, additional costly, power-hungry and space-hogging circuits, such as transistors and charge pumps, are required. In legacy contact smart card architectures the power

source is readily available via hard-wired contacts. In passive contactless smart ICs, power is sparse and generated via radio signals. Using floating gate EEPROM and Flash technologies, passive contactless ICs have relatively long transaction times to write data. More power-efficient memory technologies can decrease transaction times while adhering to the RF passive source's limited power capacity.

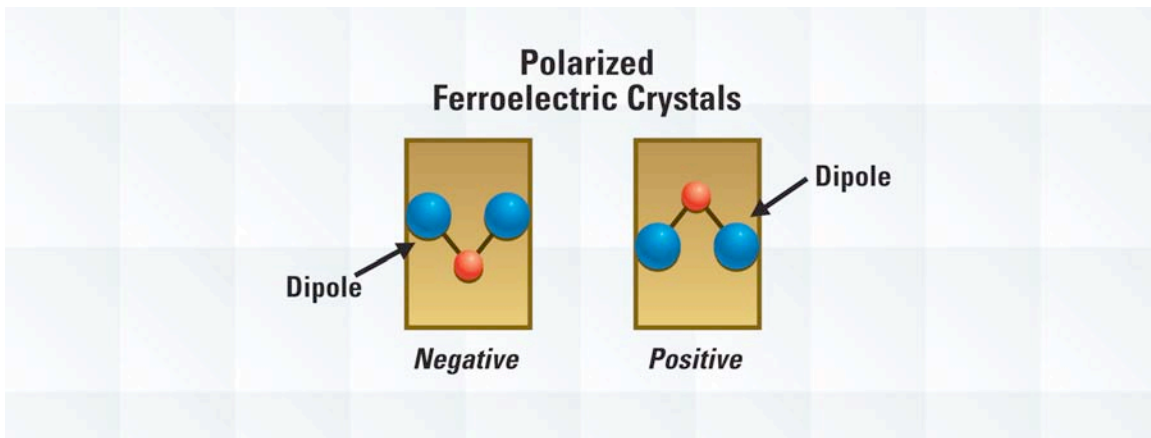
Another restriction of all the high-voltage legacy circuitry is it does not easily scale to smaller and smaller IC manufacturing process technologies, also called process nodes. The driving force behind the manufacture of ICs is miniaturization, and shrinking process nodes can take better advantage of faster computing and decreased power consumption. EEPROM and Flash memory require specially-designed high-voltage transistors, which are difficult or technically infeasible to further reduce in size, putting limitations on their ability to scale to smaller chip manufacturing process technologies.

The programming process, in which data is written to EEPROM and Flash memory by putting a charge onto the floating gate, limits the write cycle endurance of the smart IC. Future government ID applications incorporating in-the-field data writing may require a large number of write cycles in excess of what can be supported by EEPROM and Flash memories.

In terms of data security, EEPROM and Flash memory technologies are inherently susceptible to unauthorized observation. One example of an EEPROM vulnerability is when the memory is in static mode (no energy is coming in or out of the floating gate). In this state, nanoprobe can be used to scan the memory in the floating gate and if someone is physically close enough, he or she can measure the electric fields and determine the data contained in the memory location. This could potentially reveal sensitive data, encryption keys, or privileges and access rights.

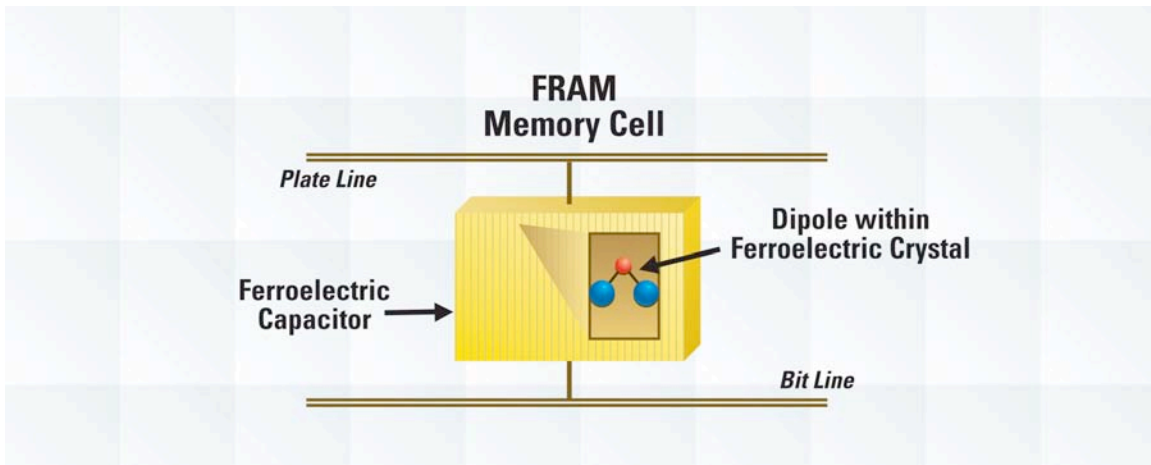
Advanced FRAM: Attributes and Benefits for Government ID

FRAM is a non-volatile memory technology like EEPROM, however the similarities end here. FRAM uses tiny ferroelectric crystals integrated into a capacitor. Although "ferro" means iron, FRAM does not contain iron. A ferroelectric crystal is a dielectric phenomenon that relates to electric fields, and therefore has no magnetic sensitivity or disruptions associated with iron. In contrast to the complex charge storage mechanism used in EEPROM and Flash, FRAM stores information through the use of a spontaneous, stable electric dipole found in the ferroelectric crystal. Intrinsically, the dipole atom within a ferroelectric crystal has either positive or negative orientation (See Graphic 1).



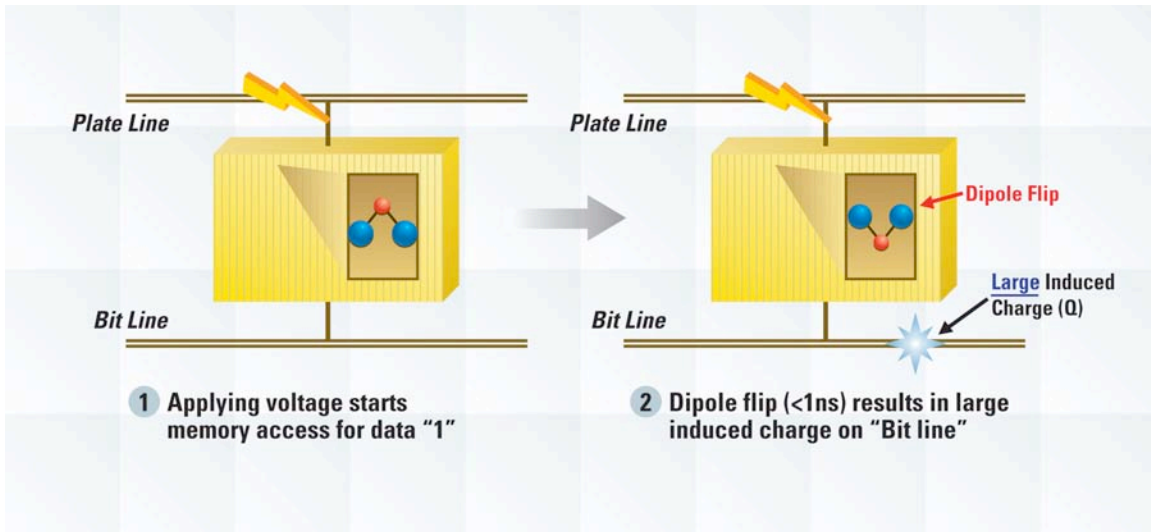
Graphic 1

An FRAM memory cell consists of a ferroelectric capacitor connected by a plate line and bit line as seen in Graphic 2. The orientation of the dipole within the ferroelectric crystals that make up the capacitor material can be set and reversed through the application of an external voltage across either line.



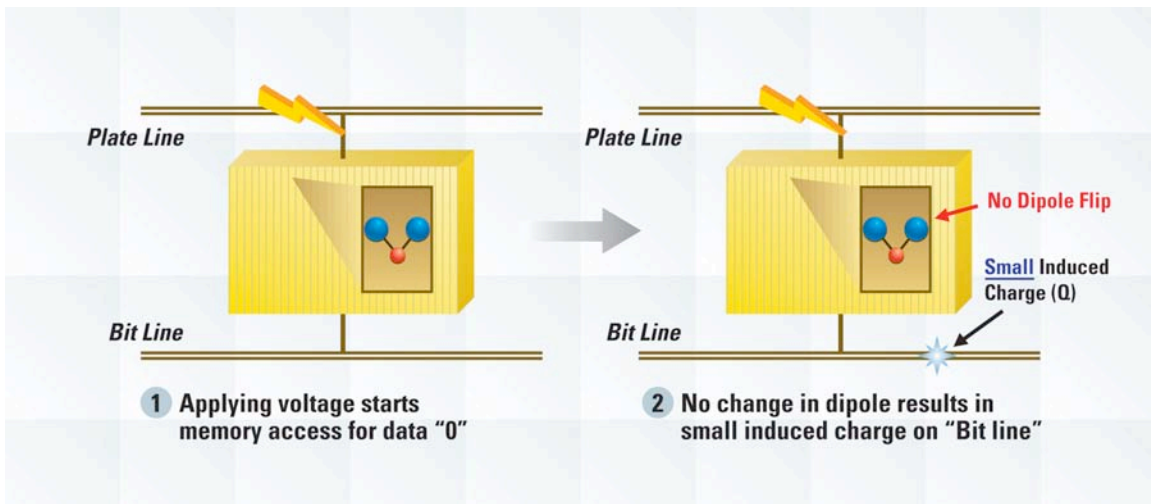
Graphic 2

To access the stored data in an FRAM memory cell, a small voltage is placed upon the plate line. If the voltage causes dipoles inside the capacitor to flip orientation, then a large induced charge (Q) is generated on the bit line, as seen in Graphic 3.



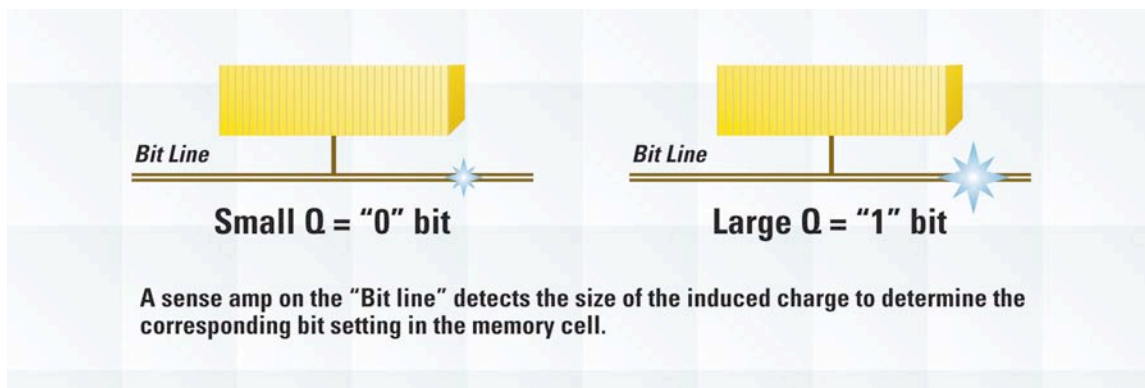
Graphic 3

When there is no change in dipole direction as voltage is applied to the plate line, then a small induced charge (Q) is created on the bit line – as in Graphic 4.



Graphic 4

Ascertaining "0" and "1" bits with FRAM is simply determined by the size of the Q induced charge on the bit line (See Graphic 5).



Graphic 5

To refresh or write new data to an FRAM memory cell, the dipoles are easily oriented positively or negatively via an applied voltage to either the bit line or plate line. The dipole flip occurs rapidly, in less than one nanosecond (<1ns), enabling fast read and write access to the memory. The ease and speed by which data is established within an FRAM memory cell illustrate the shift away from the design complexity of EEPROM and FLASH floating gate technology to the natural phenomenon that is inherently available within a ferroelectric crystal.

The orientation change of the dipole occurs extremely fast. Therefore, it takes dramatically less time to write to FRAM devices than those using EEPROM and Flash. FRAM memory cells can be written to in less than 50 nanoseconds, compared to microseconds or milliseconds for EEPROM and Flash, making FRAM 1,000 – 10,000 times faster than these older memory technologies. Once the ferroelectric is in either a positive or negative state, it stays there, even when the electric field is removed, meaning that FRAM has long data retention. Even at high temperatures (at 85 degrees Celsius), FRAM retains its data for more than ten 10 years. FRAM can also be accessed for more than 100 trillion write/read cycles, or virtually an inexhaustible amount of times.

A high electric field is not required to switch the dipoles, enabling FRAM to use a low voltage of 1.5 volts to write and read data. Low voltage, which translates to low power usage, has other benefits. First, high-voltage transistors aren't required, nor is there a need for high-voltage circuitry, such as charge pumps, to boost the voltage higher. Second, because only a small amount of energy is required, all the necessary power for FRAM can be front-loaded at the beginning of a write cycle. This avoids "data-tearing," a partial write of the data which occurs when the smart IC is removed from the RF field power source during a write cycle. EEPROM and Flash are more prone to data tearing. Therefore, low voltage and power usage of smart ICs with embedded FRAM offer enhanced data integrity and an improved user experience.

Other inherent advantages of FRAM include protection against direct data security probe attacks (described in the previous section) and radiation hardness. As a response to anthrax threats, gamma radiation is used at some U.S. Postal Service locations on a regular basis. Compared to traditional non-volatile memories, FRAM is significantly less

susceptible to gamma radiation, thus special handling would not be required when shipping FRAM-based electronic documents such as e-passports.

FRAM and the 130 Nanometer Chip Process Node

Process technology refers to the particular method used to make silicon chips. The size of the features (e.g. the elements that make up the structures on a chip) are measured in nanometers (nm), which is one-billionth of a meter. For comparison, the diameter of a human hair ranges from 80-180 millionth of a meter. A 130 nm process technology or node refers to a silicon chip with features of 130 nm or 0.13 μm in size.

Compared to the 180 nm process node typically used to make smart ICs, twice the amount of circuitry can be placed on the chip in a given unit area using the 130 nm process node. By producing FRAM at 130 nm, more memory can be placed within smaller ICs using less power than can be achieved using traditional embedded memory technology approaches. Table 1 contrasts embedded FRAM produced at 130 nm to typical EEPROM and Flash embedded non-volatile memory technologies for passive devices.

Non-Volatile Memory Comparison

	FRAM	EEPROM	Flash
Time-to-program 64 bytes to memory	1.6 μs	2200 μs	6400 μs
Voltage applied to memory cell to write	1.5v	10-14v	10-14v
Impervious to data-tearing during write	YES	NO	NO
Number of possible write cycles	100 Trillion	500,000	100,000
Time-to-read 64 bytes from memory	1.6 μs	4.5 μs	4.5 μs
Resistant to gamma radiation	YES	NO	NO
Mask adders in low-voltage IC production	2	7	6

Table 1

Creation of ICs using FRAM is also more efficient because the extra mask steps associated with creating the high-voltage devices are eliminated. Adding EEPROM or Flash capability to integrated circuits requires additional process steps and approximately five to eight added lithography masks. In contrast, embedded FRAM at 130 nm requires only two additional masks.

FRAM's fast access time, low power dissipation, small cell size, and efficient manufacturing process, which is scalable to smaller and smaller process nodes, mean it is well-suited for next generation contactless smart ICs.

FRAM's Impact on Government ID Production Processes

The creation of a government-issued electronic ID document adds a substantial level of complexity to the production process of the credential. Not only are electronic components integrated into the document, data must be written to the smart IC. There are two primary steps in the writing process: pre-personalization and personalization.

Pre-personalization is the process by which the smart IC's on-board memory and/or Operating System (OS) are formatted for the particular application (similar to formatting a computer disk). In a typical process to create a government electronic ID document, such as an e-passport, the pre-personalization step is done by contactlessly writing the formatting information to several credentials on a single sheet of substrate material at the same time. Writing pre-personalization data to chips is done in bulk for the sake of efficiency. Slow chip write times, in conjunction with chip performance variability, can affect how a chip is formatted. If any one of the smart ICs is improperly formatted during pre-personalization, the "bad" chip will continue in the process until all of the credentials are made into finished products.

Poor RF chip sensitivity can also increase the likelihood of yield problems during production of the credential. A less sensitive chip does not perform well relative to others when RF signals between the reader and chip are weak or are temporarily affected by an external source. Even a small percentage of improperly pre-personalized chips can have an enormous effect on production cost because some products will need to be scrapped at the end of the entire production process.

Once the document has been completely assembled, formatted and manufactured into individual credentials, then personalization of the chip takes place. During personalization, the credential holder's personal data is loaded onto the smart IC.

Using EEPROM and Flash memory, the transaction time to write all of the data the smart IC during both pre-personalization and personalization can significantly slow the electronic document production process. Production time can be greatly reduced by the use of smart ICs with embedded FRAM. A smart IC with robust RF sensitivity and fast memory write speeds, such as those that incorporate FRAM, can make a tremendous impact on the production time, cost and quality level of electronic government-issued electronic IDs.

Access Control and Security

Ever-increasing security demands place constant pressure on government agencies to deploy stronger levels of security in government-issued credentials. Although large-scale issuance of e-passports began in 2006, preparations are already underway to increase security. To accommodate higher levels of security, smart ICs contained in these IDs need to scale to hold more data and must also have fast transaction speeds to write and read this data.

BAC and EAC in Electronic Passports

The RF-based contactless smart card IC in today's e-passports has a number of security features. One such measure established in the ISO/IEC 14443 standard is a short reading distance of 10 cm (4 inches) or less between the chip and RF reader. All current e-passports also have Basic Access Control (BAC) security, a criteria developed by the International Civil Aviation Authority (ICAO). The information stored on the chips of today's e-passports with BAC is the same as on the printed data page, plus the digital photo. BAC requires that the machine readable zone on the data page be read electronically by the reader first to unlock the chip. Once the chip is unlocked, it then transmits the passport's number, individual's date of birth and the digital photo of the passport holder, back to the reader via encrypted communication. BAC was adopted to minimize the risk of eavesdropping, intercepting the electronic information that moves between the chip and reader, and skimming, obtaining data from the passport holder surreptitiously.

There are efforts underway to increase security on the e-passport to ensure the passport holder is the credential owner. This requires more sensitive information than a photo (such as fingerprint or iris biometrics) be added to the chip. ICAO recommends the use of Extended Access Control (EAC) to protect fingerprints and other sensitive biometric data such as iris scans. European Commission regulation EC 2252/2004 calls for the incorporation of fingerprint data on European Union e-Passports by June 28, 2009.

EAC performs BAC, plus smart IC authentication and terminal authentication. Smart IC authentication is the act of proving the smart IC is genuine to protect e-passports from cloning, while terminal authentication is the act of proving that a reader is a genuine reader, as well as ensuring that the e-passport's chip will not provide its information to an unauthenticated reader.

The Effects of BAC and EAC on IC Memory, Processing Speed and Security

The complexity of the infrastructure to support second-stage biometric data and EAC places greater demands on smart ICs; they need to have increased memory capability, faster processing power and new levels of security. Most e-passport solutions using BAC currently require less than 32 kilobytes (KB) of memory while up to 125 KB is expected

to be initially needed for EAC (5KB for machine readable zone and other basic data; 20 KB for a facial image; and 10 KB per fingerprint image). The amount of data required for EAC will have a big impact on productivity when e-passports are personalized. Personalization time for EAC will increase dramatically using chips with EEPROM and Flash memory as almost twice the data will need to be written to the chip for 2 fingerprints (an increase of 25 KB to 45 KB). The chip must be read to verify the data after it is initially written, further adding to increased production time. In addition, doubling the amount of data read from the IC to authenticate the e-passport holder's identity will also increase inspection times at border checkpoints.

New Government ID Applications Require an Advanced Smart IC

New government identification applications, including the next generation of e-passports and multiple-application National ID cards, will demand a more powerful and efficient smart IC with improved memory capability and faster data access speeds. First generation e-passports marked the beginning of the migration away from a paper-based document. Future versions, with fast write and read times and more memory, could efficiently employ additional functionality such as entry/exit location information and electronic visas, which can be written to the IC on the fly. This electronic-based data provides increased protection at the border by giving inspectors access to an instantaneous history of where the person has been, or flagging them if a person's visa is expired. The inspector wouldn't have to look through the pages of the passport book to get this additional information, potentially slowing down the process. Data on an e-passport, when properly secured, has the advantage of being less susceptible to fraud than hand stamping, and using a capable secure smart IC, won't slow border inspection.

National citizen and governmental agency ID cards may hold multiple applications. To link additional applications to an individual's credential after it has been issued, requires new data be written to it. For example, if the health services agency issues a contactless smart IC-based card to an individual and later the pension agency wants that person to use that same card, then the pension agency will write its application data onto that same credential. To prevent a lengthy wait to upload the application onto the credential, the smart IC needs fast writing speeds to reduce processing time. If applications are automatically written or removed at a consumer terminal or kiosk, faster chip speeds can cut queue lengths and wait times.

The Homeland Security Presidential Directive (HSPD) - 12, and corresponding Federal Information Processing Standards (FIPS) 201, are other examples of the need for a next-generation smart IC. The DOD has issued FIPS 201-1 Personal Identity Verification (PIV) cards, and several other federal agencies have started to deploy the new credentials. Designed to enhance security, reduce identity fraud and protect privacy, HSPD-12 establishes a government-wide standard for secure identification credentials used by the U.S. Federal Government and its employees and contractors. Today, the ID cards have multiple uses for both physical and logical access control, but because they are contact-based, they do not permit biometric data to be transferred via RF communication. More

efficient smart ICs could handle the additional security to allow contactless biometric data transmission while also enabling quicker personalization and card issuance. Further, as with e-passports, there is an opportunity to incorporate electronic location stamping using the fast processing speed of new smart IC technology.

Another capability being evaluated for government ID credentials is biometric match-on-card security. Match-on-card technology uses biometrics as a Personal Identification Number (PIN) replacement in access solutions by performing the actual fingerprint match within the secure smart IC card environment. This removes the uncertainty of matching the fingerprint to a database, via a network-connected device, or external server, typically considered weak links in the chain of security. Privacy concerns can be addressed by having the user control the association of his or her biometric information to the credential. The ability of smart ICs to quickly access and process this biometric data on the chip is critical in reducing user wait times and eliminating queues for match-on-card applications.

Texas Instruments' Approach to Government Electronic ID

Texas Instruments is creating a next-generation smart IC platform developed specifically for the government ID market. It will employ advanced memory technology called FRAM, and it will be manufactured on the state-of-the-art 130 nm process. Since 2003, TI has produced hundreds of millions of ICs at 130 nanometers using industry-standard CMOS processes. TI's use of the latest 130 nm manufacturing node results in chips that are much smaller than the 180 – 220 nm node sizes used by most other RF contactless manufacturers, giving TI significant advantages in terms of size, cost, and power efficiency. By moving to a 130 nm process, TI will create FRAM memories within its CMOS manufacturing process using the smallest commercially available FRAM cells shown to date.

TI's smart IC platform will feature extremely fast write and read times. Government-issued electronic IDs will be produced, personalized and processed more quickly and efficiently thus reducing life-cycle costs. TI's smart IC platform will contain the memory and processing performance to accommodate current and future security and encryption requirements. In addition, it will address new capability requirements added to future versions of government IDs such as multi-application documents or write on the fly data, including entry/exit location information and electronic visas.

About the Authors

Joseph Pearson

**Government Identification Marketing Manager, RFid Systems
Texas Instruments**

Joseph Pearson is a government identification marketing manager for Texas Instruments. In this role, he is responsible for developing market opportunities associated with government-issued documentation such as passports, border crossing cards, government benefits cards and other multi-application smart cards. Throughout his 16 years within TI, Joseph has held a variety of instrumental positions in sales, marketing, and business development. Most notably he played a pivotal role in the technology and patent development for what became the ExxonMobil Speedpass™. Prior to joining the government identification team, Joseph led business development initiatives for TI's authentication and pharmaceutical team which is responsible for RFID asset tracking across a variety of industries. Joseph has been instrumental in the development of several RFID patents.

Joseph holds a B.S. degree in Economics and Business Administration from the University of Nebraska, Lincoln, NE, and serves on the Board of Directors for Eagles Wings Retreat Center, a non-profit youth retreat center located in central Texas.

Ted Moise, Ph.D.

**Non-Volatile Memory Department Manager
Mixed Signal Technology Development
Texas Instruments**

Ted Moise is a distinguished member of the Texas Instruments technical staff and is currently the non-volatile memory department manager within the company's mixed-signal technology development organization. Ted has authored or co-authored more than 60 papers, served as conference and session chair for several international technical conferences, presented numerous invited lectures, and holds more than 30 issued patents.

In 1997, he and his colleagues at TI started work on the development of embedded ferroelectric memory devices and circuits. This group demonstrated the first operation of low-voltage, high-density, embedded ferroelectric memory in 2002. In conjunction with Ramtron International Corporation, this group has also produced the first high-density (4Mb) ferroelectric memory product on an advanced (130 nm) silicon technology node.

Ted earned B.S. degrees in physics and engineering from Trinity College, Hartford, CT, and his Ph.D. in electrical engineering from Yale University. While at Yale, he earned the Harding Bliss prize for excellence in engineering and applied science.

About Texas Instruments

A technology pioneer in secured contactless applications, Texas Instruments delivers many innovative contactless and secured products to the forefront of the electronic ID and payments markets. ExxonMobil's SpeedPass™ and the American Express Blue Card leveraged TI's technical expertise in providing the first "pay-at-the-pump" application and the innovative clear contactless credit card design. TI is developing faster, more secure smart IC applications for the next generation of contactless electronic government-issued identification. High-performance and low-power contactless applications continue to be evidence of TI's strength in designing robust, yet streamlined products that execute more efficiently. Capitalizing on its competencies in high-volume semiconductor manufacturing and microelectronics packaging, TI is a visionary leader and at the forefront of establishing new markets and international standards for secured contactless applications. For more information, call 1-800-962-7343 or visit the Web site at www.ti.com/govid.

Texas Instruments Incorporated provides innovative DSP and analog technologies to meet our customers' real world signal processing requirements. In addition to Semiconductor, the company includes the Education Technology business. TI is headquartered in Dallas, Texas, and has manufacturing, design or sales operations in more than 25 countries.

###