# BIOMETRIC PROTECTION OF SMARTCARDS THROUGH FINGERPRINT MATCHING: A TECHNOLOGICAL OVERVIEW AND POSSIBLE DIRECTIONS

**Evangelos D. Frangopoulos [1,*] and Lucas M. Venter [2,**]**

[1] Electrical Engineer (M.Sc.) / Postgraduate Student, Department of Computer Science and Information Systems, UNISA.

[2] Professor, Department of Computer Science and Information Systems, UNISA.

[*] 40B, Mohamed Mazhar, Zamalek, Cairo, Egypt.
Tel.: +20 10 639-6819. eMail: vfrangopoulos@hol.gr

[**] TvW 8 Theo van Wijk Building, UNISA, Muckleneuk Pretoria, South Africa.
Tel.: +27 12 429-6368. eMail: ventelm@unisa.ac.za

## ABSTRACT

In recent years, numerous developments in Smartcard Technology have allowed smartcards to be used as a secure means of identification and authentication, as well as encrypted data carriers and processors. Smartcards can be found in a great variety of security-related applications ranging from (but not being limited to) security access tokens to mobile phone SIM cards to conditional access decoding modules for satellite and cable broadcasts.

Traditionally, smart cards have been protected by passwords so that their use by unauthorised persons is prohibited. However, traditional passwords can be shared, stolen or intercepted, thus ultimately compromising the security of the smartcard.

Recent and expected advances in a variety of technological fields, allow for the design of more powerful and flexible smartcards with integrated thumbprint-based biometric protection. This paper discusses such advances and hopefully provides some insight into possible future directions of smartcard design.

## KEY WORDS

Smartcard, identification, biometric, fingerprint, thumbprint scanner, cryptography, security.

# BIOMETRIC PROTECTION OF SMARTCARDS THROUGH FINGERPRINT MATCHING: A TECHNOLOGICAL OVERVIEW AND POSSIBLE DIRECTIONS

## 1 INTRODUCTION

Smartcards have been around for approximately two decades and their wide acceptance has already made them the platform of choice for all applications where user-authentication is necessary. The scope of this paper is to recapitulate on current technology and discuss the perspective of raising the security level of smartcards through the use of biometric controls. In the proposed scheme, all of the acquisition, processing and matching of biometric data (in fingerprint form) is done on the card. The paper gives an overview of the technologies -both present and expected- that are necessary for such an implementation. Although aspects of the discussion are based on potentially non-original work, the authors hope that this paper will help in laying the foundation for the systematic examination of the integration of the necessary technologies.

## 2 HISTORY OF THE SMARTCARD

The smartcard concept was conceived in the late 1960's and early 1970's. The smartcard evolved form the existing -at the time- magnetic stripe PVC card and the security shortcomings related to it. Fraud and tampering issues as well as the lack of data storage capacity and processing power were addressed by the invention of the Integrated Circuit Card (or ICC). The exact paternity of the ICC is a disputed issue but according to Petri [PET], the first ICC-related patent was filed by German inventors Jurgen Dethloff and Helmut Grotrupp in 1968. In 1970, Dr. Kunitaka Arimura of Japan filed a patent on the ICC concept [CRW]. In 1974 Roland Moreno of France further devised the concept of installing computer memory on a plastic card and thus filed the original patent for a practical ICC. This ability to install embedded integrated circuits on a flat credit card-sized piece of PVC, effectively launched the chip card industry. ICCs thus evolved from the simple cards equipped with a memory chip which were known as "memory cards", to microcontroller-based cards, today known as "smartcards".

The smartcard evolution was driven by commercial manufacturers such as Bull CP8, SGS Thomson, and Schlumberger, who began developing ICC products in 1977 [CRW]. Around 1978, Motorola, in conjunction with Bull, developed a two-chip microcontroller-based card while a couple of years later the first secure single chip microcontroller-based card was created. This was the type of smartcard that was subsequently used in the French banking system. Between 1982 and 1984 the first major ICC field test took place in France when the French Telecommunications Organisation (PTT) implemented a very successful pilot program with pre-paid telephone cards. The success of the pilot program resulted in many millions of telephone smartcards to enter circulation within two years. In parallel to the telecommunications sector, in 1984, successful field testing of smartcards within the banking sector was carried out in France with single-chip microcontroller-based ATM cards designed by Motorola/Bull [MOT97]. The ATM cards' operation was enhanced by the progress in the cryptography field that had been taking place since the 1960's. The smartcard proved to be an efficient medium for safely storing cryptographic keys and through them ensuring the safety of ATM transactions. In 1986, microcontroller-bearing smartcards entered the U.S. banking systems in volumes that exceeded 50,000 units.

In the decade that followed this early adoption of smartcards, mainly as a result of the huge success of pilot programs and field trials, smartcards proliferated in a number of fields. An increasing number of banks, mainly in the US and Europe, adopted smartcards for ATM transactions. In the US, smartcards were used by the Department of Agriculture in nationwide programs and for state-wide welfare projects. Pre-paid smartcards became available in Denmark within the framework of an "electronic purse" project. In Germany, more than 70 million smartcards were issued as citizen health cards. In France, multi-function smartcards incorporating functions as diverse as ATM-related and telecard ones were issued.

Since the mid-90's the proliferation of smartcards has been even more aggressive. Additionally to what has already been discussed, smart cards are currently used as identification and access tokens in security-related applications, as mobile telephony subscriber modules, as carriers for confidential personal health and insurance data, as pay-tv and satellite broadcast decoding modules and as pre-paid value cards, to name but a few applications. The proven large acceptance of the smartcard has led to increasing support from industry which in turn has helped the smartcard to enter even more fields of everyday life.

Technological advances have allowed the creation of contactless smartcards that use low-power radio signals for communication instead of IC contacts. Although this paper uses the contact-bearing smartcards for its discussions, the general principles can easily be extended to cover all smartcard types.

## 3 SMARTCARD CORE TECHNOLOGY

Smart cards are usually made of PVC. PVC is the preferred material of construction because it offers a reasonable amount of flexibility that adds to the endurance of the smartcard.

Smartcard construction today is governed by the ISO 7816 standard. This standard was partly based on the pre-existing ISO 7810 standard that governs magnetic stripe cards such as credit cards (thus the similarity in size and thickness between standard credit cards and IC cards in general). The ISO 7816 governs all physical and mechanical aspects of smartcards, including contact placement that allows the existence of a magnetic stripe as well as embossing on the smartcard. The ISO 7816 standard also governs other aspects of the smartcard, among which are software development and communication with the outside world.

Inside the PVC material of a smartcard, lies embedded a single silicon integrated circuit chip with memory and microprocessor (also known a "micromodule"). The micromodule communicates with the outer world via a set of eight metallic pads on its surface, the size, placement and function of each are governed by the same ISO 7816 standard.

It has to be clarified that when the first phonecards were put to the test in France, their design -especially as far as the placement of the IC contacts is concerned- was somewhat arbitrary. That contact arrangement conflicted with the placement of the magnetic stripe present on credit and ATM cards that were of the same size. However, due to the immediate success of the phonecard pilot project, the original contact arrangement was adopted as the de facto standard for phonecards all over Europe despite its limitations.

These limitations were lifted by the adoption of the ISO 7816 standard but due to legacy systems' existence in the form of installed payphones, phonecards that do not conform to ISO 7816 may still be in use in European countries.

Out of the eight contact pads specified by ISO 7816, two are reserved for future use (RFU). The remaining six are designated as: VCC (power supply voltage), RST (microprocessor reset), CLK (clock signal), GND (ground), VPP (programming voltage), and I/O (serial input/output). It is interesting to note that only the I/O and GND contacts are required on a smartcard to meet international standards. All the others are optional.

The schematic representation of the contact pad placement appears in Figure 1 (all measurements in mm):

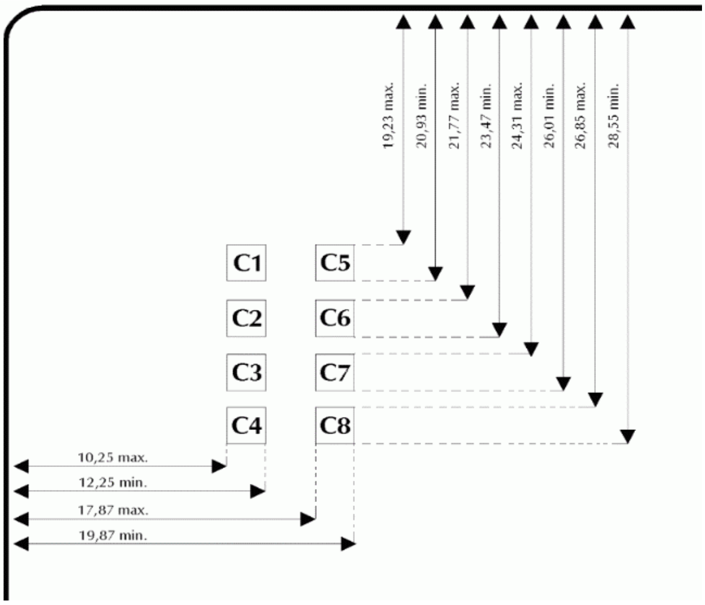

*Figure 1. Smartcard contact placement according to ISO 7816*

Conformity to the above standard is obviously paramount if any smartcard is to be read by any card reader (also known by the more formal term "Card Acceptance Device" or CAD). CADs can be designed in many ways as far as making contact with the smartcard is concerned, but in all cases, a set of eight metallic pins will have to accurately be placed on top of the smartcard's corresponding pads and electric contact be made. When a smartcard is inserted into a CAD, it is reset and proper handshake follows for communication between the CAD and the smartcard to be established.

As it has already been mentioned, the contact pads allow the embedded IC to communicate with the outside world. This IC typically comprises: a) a microcontroller or microprocessor unit which is essential for the execution of the programmed code supported by an I/O controller whose function is to control the communication between the microcontroller and the CAD, b) Non-volatile ROM memory (or any type of EPROM for development purposes) which contains the operating system of the smartcard and the executing application, c) Volatile RAM memory for use as temporary storage space and d) EPROM memory for data that needs to be stored on the smartcard by the executing application and be available after power to the smartcard is cycled.

In addition to the above, the IC embedded in certain smartcards includes a cryptographic co-processor that enables the smartcard to perform complex cryptographic operations and support public-key cryptography systems.

## 4 DESIGN ISSUES FOR STRONGER SMARTCARD SECURITY

The objective of this paper is to propose ways in which state-of-the-art smartcards can be designed for a higher level of security. The feasibility of such a scheme will be examined.

Largely due to their cryptographic capabilities, smart cards ensure the secrecy of the data they carry and thus provide a secure means of authentication for the person carrying them. This satisfies one condition of the authentication process that can be phrased as “what one possesses”. By adding a personal identification number (or PIN) which only the legitimate user of the card knows, the smart card is further protected from unauthorised use since one more condition, the one of “what one knows” is added. The obvious next step is to add biometric protection to the card in order to “match” it to its rightful owner and thus add a third condition in the authentication process, that of “who one is”.

For the above scheme to come to fruition, several technologies must be amalgamated on a single smartcard:

First, efficient protection of the contents of the smartcard must be achieved through Public Key cryptography. To this end, cryptographic co-processors are already being included in smartcards.

Second, the card must become able to capture a fingerprint image. Smart cards are already being used as biometric information carriers for larger systems but they, still, lack the ability to capture fingerprint data. While fingerprint data can be captured off-card and stored on (or retrieved from) the smartcard via a secure communication channel to the CAD, for reasons that are discussed later in this paper, it is desirable for the smartcard to be self-sufficient in this respect. This desired ability relies on the availability of fingerprint acquisition sensors of minimal size that can be placed on the card. These are being developed and their size factor and power requirements are constantly being diminished.

Third, in order to further strengthen the self-sufficiency of the smartcard, it must be made possible to process the captured data on-card. This can only be so through the use of computationally-efficient fingerprint extraction and processing algorithms, given the resource-constrained environment of the smartcard.

The combination of the above technologies, clearly, raises the computational burden that the smart-card must be able to carry in order to securely complete the fingerprint matching sequence. This issue can be dealt with, in two ways: first with the introduction of more powerful smart cards and second, with the implementation of even more efficient fingerprint-matching algorithms.

One can safely assume that a platform capable enough for the proposed implementation, if not already available, will soon be. This expectation is justified by the great acceptance of smart card technology in all fields of identification, authentication, billing, critical information storage etc. This general acceptance provides the driving force behind continuous development of smart card-related systems, products and techniques.

Thus, a smartcard implementation resulting from the combination of the above technologies, will provide a solid foundation for even more secure, smartcard-based authentication practices.

## 5 OVERVIEW OF THE PROPOSED SYSTEM

The proposed biometric-protected smartcard should be based on a standard PIN-protected smartcard equipped with a cryptographic coprocessor. The biometric data of the authorised fingerprint must be securely stored on the smartcard and never released to the outside world. A fingerprint scanner on the card must be capable of acquiring the user's fingerprint data every time the card is to be used. Through the use of efficient fingerprint-matching algorithms, a comparison of the freshly acquired fingerprint to the stored reference value will be carried out. Finally, only if the fingerprint comparison yields a match, and the PIN is entered correctly, the sensitive information necessary to further allow the transaction, will be released to the CAD.

One key issue that needs to be stressed is the need for on-card capture and matching of fingerprints. There already exist systems where the host (encompassing the CAD) provides a fingerprint scanner that is used to acquire and process fingerprint data at the time of the authentication, matching it to the reference value stored securely on the smartcard. The communication between the host and the smartcard is done over a cryptographically secure channel. However, at some point during the authentication process, the reference value stored on the smartcard must be passed to the host.

Thus, one serious disadvantage of this system architecture is that fingerprint data may be compromised by directly attacking the host responsible for authentication, and intercepting either the scanned or the reference fingerprint value.

To put the above argument into perspective, it should be considered that it is already "standard practice" for personal information and PIN codes to be intercepted at compromised ATMs around the globe. The techniques used for such purposes vary from the truly simplistic to the very sophisticated, but share one characteristic in common: ingenuity! From fake ATMs to concealed wireless mini cameras that record PIN entry, to magnetic stripe readers cleverly inserted in the scanning path of the card, to combinations of the above (and many other methods), all corroborate to the fact that no one can really take for granted the integrity of any authenticating host, especially those that are accessible by the public.

By analogy, the designer of the proposed system has to assume that the security of the authenticating host can (and eventually will) be compromised.

One could argue that by just scanning a fingerprint on the host, sending the scanned value to the card, carrying out the fingerprint-matching procedure on-card and then having the card send back a "pass" reply in case of a positive match, the host will never need access to the reference value and that this value will never leave the smart card. However true this may be, the “pass” reply sent from the card to the host, indicates that the freshly acquired fingerprint is matched to the reference one and although different from the reference value can still be malevolently used.

Thus, assuming that the smartcard is self-sufficient in performing all of fingerprint capture, processing and matching, the sequence of events should be as follows: First, a secure channel of communication between the card and the authenticating host will be established and the card itself be authenticated. Once this is achieved, an efficient algorithm running on the card will compare the fresh fingerprint image acquired by the on-board scanner, to the securely stored reference value. The outcome of the comparison (pass/fail) will be the only information that will be (securely) communicated to the host. This, in conjunction with the PIN being entered correctly, will allow the transaction to proceed.

On the issue of secure communication and storage of information, currently, RSA-based schemes implemented on smart cards are used mainly for authentication and signing. The prevailing practice is to never release the private key to the host system responsible for authentication. This is accomplished by having the smartcard do all the cryptography. This obviously constitutes a very safe method since the security of the private key is not compromised by an insecure host. One drawback of this scheme is the very heavy burden placed on the card itself since the card's infrastructure must be able to perform all the necessary cryptographic functions related to digital signatures, key generation and session encryption key exchange and unwrapping. Due to the generally constrained environment of the smartcard, specialised cryptographic co-processors embedded on smartcards take a large portion of the computational burden. This advance, allows smartcards to perform on-card RSA key generation, RSA signing and unwrapping of RSA-encoded session encryption keys. When the advances in smartcard technology and speed allow it, even real time on-card decryption of encoded messages will be possible. Still, even the simplest of these tasks are not easy to perform and adding biometric protection to them, only makes the job more difficult.

The issue of performing fingerprint matching on the card by comparing a reference value that is securely stored on the card and a freshly scanned image supplied by the host, has already been dealt with. Efficient algorithms have been devised that allow this matching to be precisely carried out in the constrained environment of the smartcard. Although there are still problems with respect to the accuracy of matching algorithms, the best of which are susceptible to an error rate of 1-2%, it seems that even at this error level, the technology is acceptable, while continually being improved [HAO]. Furthermore, the existing commercial implementations of on-card matching algorithms -such as those offered by Precise Biometrics (www.precisebiometrics.com)- provide practical evidence that the technology has already matured.

The fact that the algorithms for efficient cryptography and on-card fingerprint-matching do exist, is indicative of the notion that very soon, the two technologies will be combined to provide the desired functionality, based on a powerful enough smartcard design.

Another issue is the hardware necessary that will allow on-card fingerprint scanning. Several miniature scanner devices have recently come to existence that could readily be embedded on smartcards. These come in the form of ultra-thin full-area thumb-scanner plates, miniature swipe sensors and even self-contained scanner units that are completely self-sufficient in performing fingerprint capture and matching.

Although the obvious next step is to combine the above technologies on one smart card that will require both a PIN-type password and a biometric data match in order to proceed with the card's function, there does not seem to be a complete solution available at this time. Several angles of the problem have been tackled but none of these addresses the problem in its fullest form as described above. Along those lines, some commercial products have already been announced but the degree to which they can meet expectations, remains to be established.

## 6 CURRENT STATE OF RELATED TECHNOLOGIES

The details behind current commercial implementations of the described "building blocks" for the proposed system are hidden into obscurity for proprietary reasons. It is thus decided to present those implementations along with the theoretical background that is readily available in the form of publications. Although fairly recent, this background may be considered somewhat dated given the rate of advance of the technology related to smartcards. However, this combination of theoretical background and presentation of commercial implementations, assists in giving the reader a better and more complete picture of the current technological status.

On the issue of cryptographically-enabled smartcards, the computational burden involved, points to two different but arguably combinable directions. The first direction points towards building more power into the smart cards in the form of special cryptographic co-processors. The second direction is that of “lightening the load” for non-coprocessor-supported cards by devising clever variants of the RSA algorithm or implementing totally different ones such as the Elliptic Curve Cryptography (ECC) scheme, which is computationally much lighter and claimed to be as safe as its RSA counterpart. The second route is adopted primarily by those who feel that the increase in cost of the smart card caused by the inclusion of an arithmetic co-processor, is highly undesirable. Obviously, nothing forbids the implementation of more efficient cryptographic algorithms on specialised co-processors. Furthermore, these co-processors and algorithm do not have to be RSA-based. However, RSA-based technology seems to currently have an edge over competing public-key cryptography techniques.

Typical of the co-processor direction is the implementation of the RSAγ chip [GRO00]. The RSAγ chip provides live proof that especially designing a multiplier chip around an efficient RSA algorithm can yield decryption rates of the order of 2Mbit/s. This development undeniably paves the way for real-time decryption of RSA-encoded messages. The RSAγ crypto chip is designed with the Chinese Remainder Theorem (CRT) in mind. The chip is capable of either carrying out one straight 1024-bit modular exponentiation or two 512-bit exponentiations in parallel in CRT mode. Its flexibility and scalability with respect to multiplier word size and modulus length are of paramount importance, since the only limitation for attaining increased word size capabilities is the current technical limitations in IC construction, primarily the availability of silicon area.

According to [HAN00], the trends in the development of cryptographic co-processor design lead towards more powerful implementations of these chips. These include increases in RAM and EPROM sizes, faster internal clocks, improved security features such as address scrambling and growing public modulus sizes. The performance of these arithmetic co-processors is enhanced through the use of the Chinese Remainder Theorem and as a consequence, the time required for 1024-bit RSA signature generation is typically in the order of one second. Signature verification, on the other hand, is also sped up through the use of small exponent techniques. Another interesting technique described in [HAN00], is "size-doubling" (w.r.t. key size). According to this technique, a chip that is intrinsically capable of handling e.g. 1024-bit key lengths, is enabled to handle 2048-bit keys. Although it is beyond the scope of this paper to dwell on the details of such techniques, the interested reader is urged to study the relevant publication.

One reasonable question that arises from the study of the above information is whether the improvisation and subsequent implementation of more efficient algorithms is still safe compared to the original RSA algorithm. An answer to the question can be found in [CIE02] where known attack methods are applied against algorithms such as the RSA Multiprime scheme. This scheme, among others, is based on the use of the Chinese Remainder Theorem for decryption as well as the use of short private exponents. The results presented in [CIE02] indicate that there is a lower bound to the size of the private (secret) exponent if the algorithm is to withstand attacks. An increased number of prime factors also helps defend the algorithm. In conclusion, it seems that if certain guidelines are followed in the implementation of the examined type of efficient RSA algorithms, there should be no particular integrity problems. Hence, the described cryptographic co-processors which are designed around these algorithms can be considered safe (at least until there is sound evidence to the contrary).

Prime examples of commercial implementations of cryptographically-enabled smartcards are produced by RSA Security Inc. (www.rsa.com). Such a card is the SecurID 5100 smartcard. This card is based on Java 2.1 technology and incorporates a cryptographic coprocessor. Details for the card can be found on the relevant web page at: http://www.rsasecurity.com/products/securid/5100SmartCard.html .

The facts and insights provided in both [GRO00] and [HAN00], although somewhat dated, clearly drive home the point that there is a lot of activity in the area of cryptographic co-processor design. This trend can only be justified by the force behind it, which is none other than the high level of acceptance of the smart card as a useable cryptographic token. It can thus be readily assumed that what was described in 2000 as cutting edge technology, today is part of consumer equipment and the effort for more powerful devices is continuously gaining momentum.

The second building block for the proposed system is that of fingerprint matching. An example of the ongoing effort for smart card implementation of fingerprint matching algorithms can be found in [GIL03]. Of course, the critical issue is, again, the efficiency of the algorithm used for fingerprint matching. According to the authors of [GIL03] a sufficiently "light" matching algorithm can only be implemented on-card provided that there exists external equipment that serves as a fingerprint scanner and pre-processor. This argument is already becoming out-of-date as miniature scanner modules that can be mounted on smartcards are already appearing (more on this, to follow).

A "match-on-card" algorithm designed for commercial use on smartcards has been produced by Swedish company "Precise Biometrics" (www.precisebiometrics.com). Their "Precise BioMatch C" library and "Precise Match-on-Card" software products are designed for the confined space of a smartcard in such a way that "the (fingerprint) matching takes place in the sealed and tamper-proof environment of a smartcard".

Furthermore, in an effort to produce a more flexible and secure smartcard RSA Security Inc. and Precise Biometrics have recently joined forces. It has been established that a cooperation agreement was signed between RSA Security Inc. and Precise Biometrics for implementation of the latter's biometric matching technology in the former's software. This was stated in a relevant press release dated June 4, 2003, appearing on RSA Security Inc.'s website (www.rsa.com). In that press release, although there is reference made to Java-enabled smartcards and the potential for adding biometric functionality to them, details of the proposed scheme are not given.

In addition to its cooperation with RSA Security Inc, Precise Biometrics has signed a business agreement with Siemens ICN EN SEC for implementation of the former's fingerprint matching algorithm on smartcards using Public Key Infrastructure (PKI) developed by the latter, in the context of a European defence program (http://cws.huginonline.com/P/131387/PR/200403/939930_5.html). The project will be based on fingerprint scanners external to the smartcard, also produced by Precise Biometrics.

Datakey Inc. (www.datakey.com) has also been using Precise Biometrics' proprietary fingerprint-matching technology in the production of their biometric-protected cryptographic smartcards. One particular such model, the 330m (details can be found at: www.datakey.com/products/smart_cards/products_sc_330m.shtml ), implements ten different public key function among which RSA, DSA, Diffie-Helman key exchange and MD5.

Having shown that the necessary software/hardware combination for cryptography and fingerprint matching on smartcards do exist, the only remaining component is that of the fingerprint scanner itself.

Research is well under way on very space-efficient fingerprint scanners. One such direction is pursued by ATMEL (www.atmel.com). In [ATM01], a "white paper" on the issue, ATMEL describes the principle behind a fingerprint scanner that only requires a very space-efficient sensor that has the necessary width to accommodate that of a thumb, but is only a few millimeters high. The scan is made by swiping the thumb against the scanner instead of pressing the full finger against it. This type of scanner, apart from being very efficient in terms of space, also does away with a serious security disadvantage of traditional scanners, that of a residual image of the thumb remaining on the scanner plate after the scan. With the swiping motion of the finger on the sensor, a residual image, simply, can not be formed.

A similar solution for a capacitive swipe scanner is pursued by the Swedish company "Fingerprint Cards AB" (www.fingerprint.se). Their innovative sensor is to be soon granted a patent by the European patent office, as it was announced in mid-December 2003 [FC03]. In the company's relevent web page it is explicitly stated that the scanner will be geared towards implementation on PDAs, mobile phones and, most importantly for the current proposal, smart cards. Although the exact type of implementation is not explained, given the company's name and their level of expertise in the area of miniature systems for biometric identification, it is not unreasonable to assume that any future implementation of theirs may share many characteristics with the current proposal.

Another interesting solution using a full-size scanner instead of a swipe one, is provided by Biometric Associates Inc. (www.biometricassociates.com). Their BAI Authenticator 1.6 product is a self-contained fingerprint scanner module capable of acquiring a fingerprint image, matching it to a pre-stored reference value and signalling the smartcard for the outcome of the comparison. Unfortunately, minimal detail is given for the product at the relevant specification sheet / web page (www.biometricassociates.com/docs/productsheet.pdf) and the claims made for compatibility to ISO7816 smartcards have to be taken at face value since there is no reference made to commercial products using the product on the company web site and an email request for further information has been left unanswered.

Security issues emanating from the possibility of compromising the fingerprint scanner by fooling it through the exploitation of a residual image or use of a 2-D or 3-D finger copy bearing the authorised fingerprint as discussed in [BRA02], should not be overlooked. Although exploitation of residual images can be blocked through the use of swipe sensors as mentioned above, swipe sensors can still be fooled by finger replicas. Matsumoto's techniques for creating fake "fingers" out of readily available materials [MAT02] and his team's subsequent success in fooling many types of fingerprint scanners, clearly call for effective countermeasures. In order to provide for controls against dummy fingers or even fingers that have been detached from their rightful owner's body, scanning system sensor research is directed towards enabling the sensors to determine whether a finger is alive by monitoring for blood-oxygen level, pulse, blood flow, humidity and skin conductivity as well as temperature. It is only reasonable to assume that this technology, will eventually be used in sensors appropriate for on-card implementation. However, the current state-of-the-art in sensor technology, although lacking in the context described above, is still perfectly acceptable for the scheme proposed in this paper.

All in all, the elements necessary for the implementation of the proposed scheme either exist or the drive forcing their advancement will soon yield fruit. The combination of these elements in the manner described above, is worth being investigated and formalised.

## 7 CONCLUSIONS

Hopefully, the need for a self-sufficient smartcard that is capable of performing user authentication has been made evident. It was shown that the basic building blocks necessary (both in software and hardware) for such an implementation, exist in varying degrees of completion. The internal working details of such building blocks are generally not available and this is mostly due to proprietary reasons. Although combining the described technologies is an engineering problem that is being tackled by a number of, predominantly commercial, entities, it is the strong belief of the authors that a formal approach to this issue must also be pursued.

Assuming that the proposed scheme is the reasonable smartcard security-strengthening path to follow (and the industry trends corroborate to this effect) it is necessary for this type of implementation to be formally coded at this point. This will aid in avoiding the possibility of proliferation of a plethora of similar but, at the same time, radically different and possibly conflicting approaches. The possibility of such a multitude of implementations may well have adverse effects on future standardisation. It is further conceivable that careful formal modelling at this stage can constitute the groundwork for an appropriate ISO 7816 extension.

Finally, the authors would like to thank the anonymous referee for drawing their attention to the work done in [MAT02].

## 8 BIBLIOGRAPHY

**[ATM01]:** Bishop, P. ATMEL White Paper: Atmel's FingerChip™ Technology for Biometric Security. *Atmel Corporation.*
(Available on the Internet at:
*http://www.atmel.com/dyn/resources/prod_documents/FingerChip_WhitePaper_11_12_02.pdf*
Accessed on 16/7/03).

**[BRA02]** : Brandt, A. Biometric Security Barely Skin-Deep. *PCWorld.com. 1/8/2002.*
(Available on the Internet at:
http://www.pcworld.com/news/article/0,aid,103535,00.asp
Accessed on 14/7/03).

**[CIE02]**: Ciet, M., Koeune, F., Laguillaumie, F. and Quisquater, J.-J. 2002. Short Private Exponent Attacks on Fast Variants of RSA. *Univerisite Catholique se Louvain Crypto Group Technical Report Series, Technical Report CG-2003/4.*
(Available on the Internet at:
*http://www.dice.ucl.ac.be/crypto/tech_reports/CG2002_4.ps*
Accessed on 1/8/03).

**[CRW]**: CardWerk Technologies. Smart Card Overview.
(Internet address: *http://www.cardwerk.com/smartcards/*
Accessed on 19/03/04).

**[FC03]:** Fingerprint Cards AB, Dec 2003. Fingerprint Cards′ swipe sensor method to be granted a European patent.
(Internet address: *http://www.fingerprint.se/page.asp?section=news&newsID=167*
Accessed on 18/1/04).

**[GIL03]**: Gil, Y., Moon, D., Pan, S. and Chung, Y. 2003. Fingerprint Verification System Involving Smartcard. Information Security and Cryptology – ICISC 2002. 5th International Conference, Seoul, Korea, Nov. 28-29, 2002. Revised papers. Lecture Notes in Computer Science pp. 510-524, edited by P.J. Lee and C.H. Lim. Springer-Verlag.
(Available through UNISA's OASIS at:
*http://www.springerlink.com/app/home/content.asp?wasp=43wrc22l124krj48b386&referrer=contribution&format=2&page=1&pagecount=0*
Accessed on 23/7/03)

**[GRO00]**: Grossschaedl, J. 2000. The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip. *IEEE Proceedings of the Sixteenth Annual Computer Security Applications Conference (ACSAC'00).*
(Available on the Internet at:
*http://csdl.computer.org/dl/proceedings/acsac/2000/0859/00/08590384.pdf*
Accessed on 9/8/03 through the American University of Cairo (AUC) library facilities(service requires subscription)).

**[HAN00]:** Handschuh, H. and Paillier, P. 2000. Smart Card Crypto-Coprocessors for Public-Key Cryptography, in *Smart Card Research and Applications, Vol. 1820 of Lecture Notes in Computer Science*, pp. 386-394, edited by J.-J.Quisquater and B. Schneier. Springer-Verlag.
(Available on the Internet at:
*http://www.gemplus.com/smart/r_d/publications/ps/HP00copr.ps*
Last accessed on 10/8/03).

**[HAO]**: Hao, Y., Tan T. and Wangan Y., Effective Algorithm for Fingerprint Matching.
(Internet address: *http://nlpr-web.ia.ac.cn/english/irds/papers/haoying/TENCON.pdf*
Accessed on 3/6/04).

**[MAT02]**: Matsumoto, T. 2002. Gummy and Conductive Silicone Rubber Fingers Importance of Vulnerability Analysis, in *Advances in cryptology-ASIACRYPT 2002 : 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 2002 : proceedings,* pp. 574-575, edited by Yuliang Zheng. Springer.

**[MOT97]**: Motorola, Inc., Mar 1997. Motorola Smartcard Systems Business: Technology Background.
(Internet address: *http://www.motorola.com/LMPS/pressreleases/ssbtech.html*
Accessed on 19/3/04).

**[PET]**: Petri, S. SSP Solutions White paper: An Introduction to Smart Cards. *SSP Solutions, Inc.*
(Internet address:
*http://www.sspsolutions.com/solutions/whitepapers/introduction_to_smartcards/*
Accessed on 19/3/04).