



Testimony

Advancements in Smart Card and Biometric Technology

**Christer Bergman
President and CEO
Precise Biometrics**

**Submitted to the
U.S. House of Representatives
Committee of Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and Census**

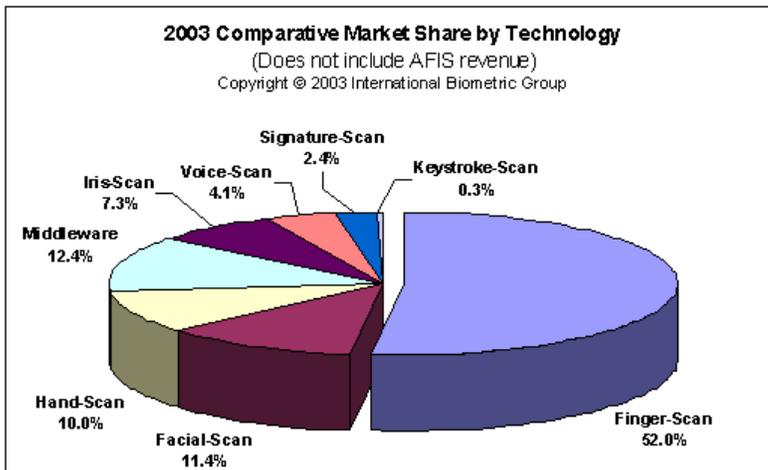
September 9, 2003

Good morning, Mr. Chairman, Ranking Member Mr. Clay and Members of the subcommittee. Thank you for the opportunity to be here today to represent the views of the industry regarding “Advancements in Smart Card and Biometric Technology” in the Federal government market.

I am Christer Bergman President and CEO of a small public company in the biometric industry, Precise Biometrics [1], our focus is fingerprint technology in combination with smart card technology. I also serve as an officer of the International Biometric Industry Association (IBIA) [2] Board of Directors. As my roles indicate, I am living and breathing “Biometrics”, an industry that is transitioning from emerging technologies into the necessary tool, which is part of our daily lives. Sadly this is in large part due to the tragic events of the last couple of years. The biometric industry today is recognized as very much in focus for Governments, organizations, corporations and individuals. But, from an industry “insider” point of view, it still needs some major “sign of approval” from Government and corporations in order to grow to a mature industry. With the above, I am delighted to have the opportunity to give an industry perspective of what is happening, what the issues are and what impediments need to be overcome in order to advance the use of biometrics and smart cards for the Federal government.

The Technologies

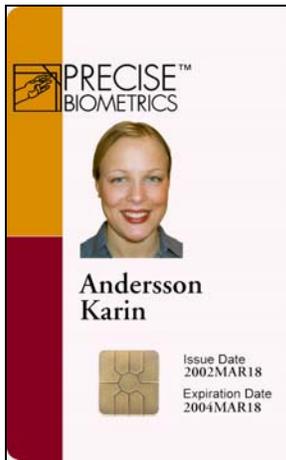
Let me start with a simple “*Biometrics 101*”. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. The characteristics measured include: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies can be used in order to identify, authenticate, or verify a person. Biometric technologies can be used as stand alone technology or integrated with other technologies such as smart cards, encryption keys, and digital signatures. The process of comparing a stored biometric template (i.e. a digital representation created from your biometric feature) with the actual captured biometric template can be done by a variety of means, computer network server, workstation, kiosk, access control terminal, embedded processor in a device, or even a processor on a smart card, known as Match-on-Card. For more detailed information about different biometric solutions, see “How secure is your biometric solution” [See Attachment].



Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. The most widely used and accepted biometric technology is fingerprint, which represents about 50% of the market today.

In the same fashion let me do a “*Smart Card 101*”; a smart card could be defined as a credit card sized plastic card with an embedded secure and powerful computer chip. The chip can either be a microprocessor based device with its own secure Operating System and internal memory or historically a simple memory chip with non-programmable logic. The Smart Card’s chip connection is either via direct physical contact or remotely via a contact-less electromagnetic interface. More and more, the smart card is being used as an intelligent ID badge, i.e. Smart ID Card. Today’s Smart ID Cards demand the highest levels of computing and security. The Department of Defense’s Common Access Card with now approximately 3Million Smart Cards deployed has been fully certified to the highest levels of security required by the US Government (NIST). The Smart ID Card can be used to access buildings, gain access to computer networks, serve as a loyalty card, a banking card and can certainly be the carrier and verifier of my personal biometric identifier(s). The microprocessor on the Smart Card can be used for many different purposes and should be viewed as a powerful and secure miniature computer with an input/output communications port, Operating System and non-volatile memory for storing information. It can also provide a secure data management system ensuring an on-board personal firewall to protect the private data maintained within the Smart ID Card from improper disclosure or usage.

The combination of smart card and biometrics can provide a very secure and convenient secure ID credential. Not only can you present something you have (the smart card), you can also present who you are (biometrics) and combined with a password (something you know); the secure ID credential then represents a very secure 3-factor authentication system. However, more often the preferred solution contains 2-factor authentication:



what you have (smart card) and who you are (biometrics). The PIN code or password is becoming a human nightmare to maintain, if we are supposed to follow all the rules regarding selecting the PIN code/password. You are not allowed to have the same PIN code for more than one application, you cannot select a PIN code that could be tracked to yourself and you have to change the PIN code every 30 days - and by the way - you are not supposed to write it down anywhere. In reality most systems today, which are based on PIN code/password, have a huge hidden security gap, the difference between how the system was designed and the practical use of the PIN code/password. Hence, in a world with a growing demand for a convenient and secure system, a biometric enabled smart card offers the best solution.

What does ***a biometric enabled smart card*** mean and how does it work? In older configurations the smart card is used only as a storage device for your enrolled biometric template captured when the card is issued to the cardholder. Upon verification, the smart card would release the stored biometric information to the workstation (or the server) and the live captured biometric template is then compared in the workstation (or server). This configuration is referred to as Match-on-PC (or Match-on-Server). The benefit is that you carry your biometric information with you and can use the biometric enabled smart card

on multiple devices that each support the same mechanism to convert the live captured fingerprint image to the corresponding template. The drawback is that your complete enrolled biometric template once transmitted by the Smart Card is exposed during transfer and verification, creating security vulnerability and a direct concern regarding the privacy of your biometric information.

From a security aspect, the more preferred configuration is when you fully utilize the capabilities of the Smart Card and use the Smart Card not only as a secure storage device, but also use it as a powerful self contained secure computer. The actual comparison of the enrolled template to the live captured template is performed within the Smart Card chip itself. If there is a match, then the Smart Card will securely supply that information to the application. This configuration is referred to as **Match-on-Card**. The additional benefit is that both the security and privacy concern will be minimized – the template verification is done within a secure environment (inside the secure area of the Smart Card) and the enrolled biometric template information does not leave the card, hence the only place your biometric template exists is within the Smart Card – which you control and carry about. Clearly the Smart Card functionality is useless to anybody else other than the enrolled person who can prove their identity by presenting their biometric for the card to internally verify.

The first biometric technology for true Match-on-Card is fingerprint technology which was introduced to the market a couple of years ago and is now a standard product offering. It can be used with most Smart Cards today and companies such as Schlumberger, Datakey, Siemens and other Smart Card manufactures have already integrated the product in their product portfolio. However, the Match-on-Card concept could be used for other biometric technologies as well.

From an end user point of view, the ideal fit for Match-on-Card is with Identity Systems that incorporate Public Key Infrastructure Technology. Instead of using the Smart ID Card's PIN code to get access to the Private key's functionality, the live captured and computed biometric template is presented and if verified with the stored template - access is granted and minimum changes are needed to the overall application and project. Both the end user and Identity System provider will experience a secure, cost effective and importantly a convenient solution to ensuring strong cardholder verification.

The Issues

What is happening?

So it seems that the combination of Smart Card and biometrics could be the optimal solution to ensure a convenient way to increase the physical as well as computer security throughout the Federal government and corporations. Why is this not happening on a broader scale?

- “We don't know how secure the system is!”
- “Integrating physical and logical security will not work!”

-
- “It costs too much – we can’t afford this!”
 - “There is no standard – it is not approved!”
 - “It is not interoperable with other biometrics systems!”
 - “Privacy concerns - my fingerprint will be available to anyone!”

These are some of the comments that you will get from the market. Let me therefore explore some of these aspects further:

Privacy.

The first misunderstanding is that people think that using fingerprint biometrics means that the system captures the fingerprint and then sends it over the (open) network, where it can be intercepted and used for criminal purposes. (Some of the science fiction movies during the recent years are good for marketing biometrics – but it does not give the complete and accurate information about how biometric technology can be used in reality). People are also afraid of being recorded in a national database involuntarily, even if they do not have any criminal record. The reality is that the Identity System uses the fingerprint to create a digital biometric template that does not show your complete fingerprint, nor can it be used to recreate your fingerprint. It is also a reality that most biometric systems today use a secure network if the biometric template is being transmitted. With the use of Match-on-Card, the biometric template does not even leave the Smart Card and you decide yourself when you want to use a service that requires the use of your biometric enabled Smart Card.

An excellent Reference paper entitled “Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems” has been published by the Smart Card Alliance and is available on their web site [3].

It should also be noted that all the members of IBIA have accepted and adhere to the IBIA Privacy Principles [2].

Interoperability.

Certainly it would be very nice if there would be complete interoperability among all the different biometric technologies – but this is not realistic. But it should be mentioned that a number of biometric implementations today include multiple biometric technologies; fingerprint + face or fingerprint + iris. Many of the biometric solutions that support multiple applications also use PIN code and other legacy technologies in order to work with the installed base of infrastructure.

Even the interoperability between biometric vendors within one biometric technology (e.g. Fingerprint) is not there today. However, there has been significant progress made over the course of the last couple of years - one of the most important initiatives is The Biometric Consortium [4]. The biometric industry is now driving towards standards, both domestic and international. However, it takes time to agree on a technical standard and as most of the other new technologies that are changing our daily life; a de-facto standard is being created in parallel with the standardization work.

The above is valid for the biometric industry and to a lesser extent the Smart Card industry, which has made significant efforts to create open standards and specifications.

However in the combination of biometrics and Smart Cards, the progress is slower largely due to the relative recent maturity of Smart Cards and their ability to now perform Match-on-Card. Therefore there is a need for visionary leadership to help create the de-facto standard for biometric enabled Smart Card technologies by funding and directing some of the ongoing Smart Card projects to include Match-on-Card biometrics as a secure, cost effective, convenient solution to strong card holder authentication.

Security of the system.

In the biometric industry, the security is often measured with the terms False Acceptance Rate (FAR), and False Rejection Rate (FRR), and the combination of the two. A biometric system could be tailored to high security (very low FAR and moderate FRR) or it could be used more for convenience (moderate FAR and very low FRR). The problem arises when comparing the FAR/FRR from different systems, because there is no standard on how to perform the tests. Should the test be done on a human population or should it be performed on a database of fingerprints, and in this case on which database? Certainly the best performance test would mirror the practical use and involve real people for the testing. One such initiative is the “Comparative Biometric Testing”, performed by International Biometric Group, IBG [5]. Another more recent development is the formation of the National Biometric Security Project, NBSP [6] whose mission includes facilitating the education, test and deployment of biometric security systems.

When it comes to comparing the security of a biometric system versus a PIN code based application, which is often the case when referring to a biometric enabled smart card - the picture becomes even more complicated. It is easy to measure the FAR for a 6 digit PIN code, where a quick calculation gives the answer 1:1,000,000. However, when the security gap (as referred to above) is taken into consideration, there is no real practical answer. On the opposite, it is only a theoretical and maximal security level. In a biometric system, it is real people in different situations who are using the system; therefore there will always be a difference in how the individual is applying the finger to the device during enrollment and verification. In conclusion, there is a need to develop test cases that mirror the real usage of a system. The results could then be used as one parameter in selecting a biometric system. Another more important parameter is installed systems and the end users feedback on the convenience aspect of the implementation.

Cost.

There are many elements that build up the cost of any system or infrastructure. Let me therefore only briefly highlight some of the considerations. If the system is a biometric only system, there is a cost per biometric device, for the biometric application and a cost for the infrastructure. Practical examples show that for a Single Sign On application, i.e. “replace my passwords with biometrics”, the return on investment could be less than 6 months. This calculation is based on the downtime for both the end user and the help desk in order to solve password problems.

If the combination of the biometrics and Smart Card is fully utilized, then the cost can be further optimized for the system as well as satisfying the need for a fully scalable Identity System. If part of the application is a biometric verification only, there is no need to have

a costly infrastructure in place. The biometric matching application resides on the Smart Card. If the Identity Verification application could be built as a “kiosk” or mobile/portable application, then there are minimum needs for biometric devices and minimum needs for connectivity to any databases storing a collection of enrolled biometric templates.

By using a combination of biometrics, Smart Card and also another new revolutionary technology; Real Time Credential, the overall cost for a project like US-VISIT would be dramatically reduced.

Overall leadership support.

Biometrics was considered a new technology a number of years ago. Very few people knew about the existence. Today there is a totally different awareness of biometrics: even President Bush, Secretary of the Department of Homeland Security Ridge and Undersecretary of Borders and Transportation Security Hutchinson frequently mention biometrics in public speeches. When it comes to smart card technology the market awareness also in the US has increased quite dramatically during the last couple of years. For strong card holder verification the combination of biometric Match-on-Card, Smart ID Cards and Public Key Infrastructure represents an ideal way to protect our Nation’s infrastructure from unauthorized access, attack or abuse.

The standardization of biometrics is on its way as well as the standardization of Smart Card technologies. However, there are very few initiatives that combine the technologies. Why is it so?

Any change of procedures, new technologies that change the way we should work or any other “disturbance” is not welcome in an organization or society. There has always been and there will always be a need for visionary leadership in order to change.

Any organization that is faced with changes has to be reviewed; this is also true for the Federal government when it comes to the combination of biometrics and smart card. The security community of the Federal government is used to the Smart Card’s “PIN code security” – i.e. all biometric systems are welcome to replace the PIN code if it can be proven without doubt that the FAR is 1:1,000,000. After the explanation above, it is obviously a good and easy measurement, however is this reality? The Biometric community has been testing systems for the last couple of years – but where are the results or directives for the industry to change or adopt? Clearly Biometric Match-on-Card is ready, tested and proven and can be deployed with confidence that strong card holder verification is practical and cost effective.

However, there are a number of organizations that have shown visionary leadership both in the government and corporations. They are implementing Smart Card and biometric systems, but they are also crossing the organizational bridges between physical and logical (computer) security. US Treasury is one such organization that realized the importance of biometrics and Smart Card and has started to build an infrastructure that can be flexible for a biometric enabled Smart Card. The DMDC and the CAC project

have shown such leadership, and are planning to take the next step in order to optimize their system and to introduce biometric card holder verification in place of, or in addition to the CAC's PIN. The State Department was one of the first organizations to implement a Smart Card based Identity System and are also showing their visionary leadership. These are only a few, there are many more who test the concept with great success, but are waiting to deploy on a broader scale. They are all waiting for any of the large Federal projects to sponsor and pioneer the new technology: the overall PKI-initiative, CAC, TWIC and/or US-VISIT.

Conclusion

Finally let me once again, express my appreciation for the opportunity to share my view on the "Advancements in Smart Card and Biometric Technology". My conclusion is that the biometric enabled Smart Card is not only a concept; it is very much a proven reality. It should lower the overall cost of a system implementation by virtue of removing the heavy support costs of PIN management, it can minimize privacy concerns with respect to storing the biometric information in a central database and the potential exposure of the biometric information when using the system. It will also optimize the usability of the overall system with respect to security and the convenience of using the biometrics for both physical as well as logical access control. The industry is actively participating in the standardization work as well as driving towards a performance test that will show real, practical performance of a biometric enabled Smart Card Identity system. However, in order to create a de-facto standard and implement a secure, cost effective and convenient security system - with a minimum of hidden security gap – there is a strong need for visionary leadership. The combined Smart Card and Biometric industries are ready and we seek your help from within the Federal government to make biometrically enabled Smart ID Cards a reality.

Thank you for your time and consideration.

Reference list:

1. Precise Biometrics, www.precisebiometrics.com
2. International Biometric Industry Association, www.ibia.org
3. Smart Card Alliance: www.smartcardalliance.org
4. The Biometric Consortium, www.biometrics.org
5. International Biometrics Group, IBG, www.biometricsgroup.com
6. National Biometric Security Project, NBSP, www.nationalbiometric.org

Attachment:

1. “How secure is your biometric solution”, Precise Biometrics White Paper