GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Being Smart with Biometrics
&
Smart Cards

By

Alan Buglass

Version 1.4b

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Abstract

This paper sets out to illustrate why using Biometrics with a Smart Card is a very secure security solution and why it is only now that these technologies are being implemented together. During the course of this document Smart Cards will be discussed, and some real life examples of where Smart Cards have been implemented will be detailed and explained. The paper will also talk about what Biometrics are, how they can be used and how they have been implemented within organizations today.

Once the Biometrics and Smart Cards have been discussed individually, the document will go on to explain why these separate technologies should be used together, and what advantages can be gained from doing this. A discussion will take place regarding current implementations of Smart Cards and Biometrics being used together, and then it will go on to talk about possible implementations for the future.

Smart Cards

In 1974 Smart Cards were conceptualized and patented by a Frenchman named Roland Moreno, but since then Smart Cards have evolved from an idea to a reality. The current form of Smart Cards has been around for more than a decade, and in that time, they have begun to be used more and more to provide security throughout organizations across the world.

Smart Cards are used a great deal within Europe, but they are just beginning to become more popular in the U.S. Smart Card Alliance conducted a study which was released in February of this year saying that 41 million cards were produced for use in the U.S last year, this was an increase of 45% from the year before.

To show how popular these cards are becoming, there have been over 1 Billion Cards produced every year since 1998, and the production rates are still increasing as more organizations look to Smart Cards for their security solutions.

A Smart Card has the size and appearance of a standard credit card, but it is a lot more powerful, a lot more secure and a lot smarter than any other type of card on the market.

As previously stated, the size of a Smart Card is the same as that of a credit card, with measurements of 85.60mm x 53.98mm x 0.76mm. These measurements are defined in ISO 7810. The ISO standard for the physical characteristics, position of the chip and exchange protocols of the Smart Card is ISO 7816.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The main standards for Smart Cards are those that are defined by the ISO (International standards Organization), but there are other organizations that are developing standards to for specific areas of the Smart Card Technology. NIST (National Institute of Standards and Technology) looks at standards related to the security of the Smart Cards in terms of cryptography. Microsoft has come up with a standard for both Smart Cards and there readers. They have called it the PC/SC specification. Visa, MasterCard and Europay have produced a standard relating to the specifications required for a payments system on a Smart Card. This proves that organizations are very serious about using Smart Cards and can see them being a facilitator in the future of their businesses.

A Smart Card is a plastic card with an integrated computer chip and a printed circuit embedded on the card. The computer chip is secured under a gold contact pad.

The diagram below shows the composition of the cards.

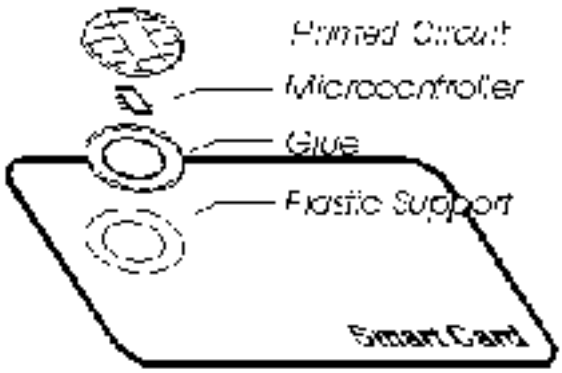


Figure 1: Physical structure of a smart card [1]

One of the main benefits of a Smart Card is that it is very self contained which means that it does not have to depend on equipment that could have had its security compromised. This enables Smart Cards to be used in areas where high levels of security are needed. One such area where this is the case is the US Air Force. The US Air Force is using Smart Cards to gain access to 100 of their bases worldwide, and 50,000 of their computers. Electronic Data Systems Corp supply the middleware and Smart Card readers for the cards.

"These smart-card readers and middleware will certainly enhance DOD (Department Of Defense) security and could play a significant role in the future of national identification cards," said Al Edmonds, president of U.S. government solutions for EDS. **[10]**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The computer chip on the Smart Card can be a memory chip, a microprocessor or it can be multi-function chip, and this is how a Smart Card is defined. The reason why an organization would choose one over the other is determined by what the organization wants to use the cards for, and the costs involved. Usually the most viable solution determined by cost is that of a single function card.

The diagram below demonstrates what organizations should consider when looking at implementing a Smart Card solution.

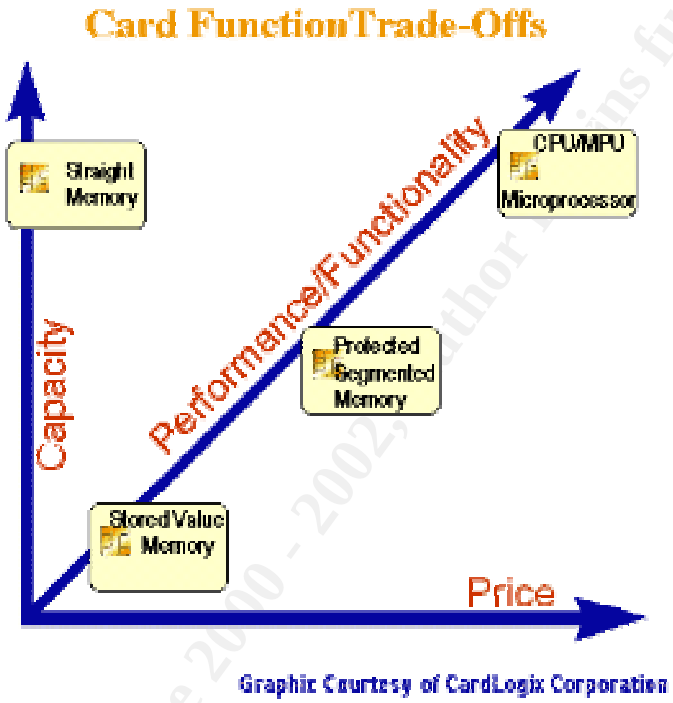


Figure 2: Price versus Capacity [5]

Another way in which the Smart Cards can be defined is by whether they are contact or contactless cards. To read a contact card, the Smart Card must be inserted into a Smart Card reader, but with contactless cards, the cards can be read via a radio link. The way in which contactless cards work is to have an antenna embedded into the card. There are also combination cards, which can use both methods to access the card.

Smart Cards are used for a number of different applications within a number of different industries. One of the main uses of Smart Cards at present is for physical access, in the way that swipe cards are used. For instance, you are able to walk up to a door hold your Smart Card in front of the sensor and the door then opens. Another use for Smart Cards is for identification, so not only can you use your card, to get into the building, but you can also use it to identify yourself to other personnel. As well as the identification and access control, Smart Cards are also used to store data in terms of digital certificates, personal details or

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

digital money. A Smart Card does not just have to be used for one purpose though; the same card could be used for all of the above and many more things besides.

There are a number of specialist organizations that work within the Smart Card arena, these include, but are not limited to Schlumberger, Gemplus, American Card Technology and ActivCard SA.

If we are to believe what these organizations are telling us, then Smart Cards are the future, in terms of a "one card fits all" solution. So instead of having an ID card, credit cards, driving license, passport etc. you would have one Smart Card. There are of course concerns regarding this, as effectively you could lose your Smart Card and someone could try and steal your identity. To stop this from occurring and to make the Smart Cards more secure Biometrics could be introduced. The use of Biometrics will be discussed later in this paper.

Smart Card Implementations

The use of Smart Cards is on the increase, and during this section I hope to give you some real life examples of how they have been implemented within various industries and organizations.

The U.S Department of Defense is going to distribute 4.3 million Smart Cards to all of its personnel including military staff, civilians and contractors. The cards are going to be used for both physical access and authenticating themselves on the computer network.

All employees of Royal Dutch Shell have Smart Cards, which are used as employee identification and also authentication for their computer network.

Sheffield Hallam University in the U.K issued Smart Cards to all of its students, and implemented an infrastructure so that the students could use their Smart Cards as digital money. They were then able to use their Smart Cards to buy various products and services around the university such as meals, stationary, photocopying and sports activities. Every time they bought something they were issued with a receipt detailing how much money was left on the card, and they could put more money on the card by inserting it in a machine and putting the amount of money in the machine that they wanted to charge it with.

The Universities of Cambridge and Nottingham in the U.K use Smart Cards for physical access, use of catering facilities, PC & web access and use of the photocopying facilities. All of the above uses for the Smart Card make it a university identity badge, but it means that instead of people having to check the card every time they enter the university or use the web, this can all be done electronically.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

American Express uses a Smart Card for one of its credit cards called American Express Blue. Stored on the card is a certificate of authenticity.



Figure 3: American Express Blue [6]

With the credit card being a Smart Card, you can actually attach a Smart Card reader to your PC and make purchases online with your card and your Pin Number. This is more secure, as you use a temporary transaction number rather than your actual account number. When you are using your card with a Smart Card reader to make payments your card and Pin Number is always required, which means that there is an extra layer of security.

As you can see, there are a lot of different uses for Smart Cards and there are a lot of different industries, which are using them. The main reason for Smart Cards being used so much now, is because of the new developments, which has increased the amount of memory, which can be placed, on a Smart Card.

Biometrics

The term Biometrics is used to describe the methods used to identify a person by using either, their physical attributes or by using behavioral characteristics. Properties that are used for identification can include face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. The most commonly used form of Biometrics is the fingerprint, as this is a tried and tested technique, which has been used for many years within the arena of law enforcement to identify criminals. New technological developments mean that Biometrics can be used in many other different areas where authentication and verification is needed. As this is the case the use of Biometrics in different industries is increasing dramatically.

In the beginning Biometrics were only used in areas where there was a very high need for security. This was due to the high costs involved and the difficulty of implementing the systems. However the costs have come down dramatically since Biometrics were first introduced, and new developments mean that implementations are a lot easier and they can be put in place a lot more quickly. The other reason behind Biometrics implementations becoming more widespread is because of the increase in attempted security breaches and fraud, which is making organizations realize that data security is a very important issue and they are now willing to invest more money for security solutions in order to protect their business.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

One might expect that people may be reluctant in using Biometrics due to privacy or concerns of data protection, but a study in the United States conducted by Columbia University reported that 83% of people approve of the use of finger imaging. This is down to the fact that people are more concerned about security than ever before as they are forever hearing about credit card fraud and people who have had their identities stolen.

However Biometrics consultant and publisher of the Personal Identification Newsletter Ben Miller says "I think the Feds love it, they think its cool, whereas if you tried to impose biometrics in a creative workplace, like Apple Computer, they might see it as Big Brother." **[3]**

Ben Miller said this in 1997, but this is still true of Biometrics today.

This is the concept of what works in one sector and improves security may be detrimental to the culture, environment and productivity within another. When implementing any security solution this is an area that has to be investigated.

The types of organizations that are looking to Biometrics for their security solutions are varied, but one of the main areas of Biometric growth is in the financial industry. This is due to the high financial loss that could occur if the strongest security measures were not in place. An example of how Biometrics is being used within a financial institution is that the Bank of Central Asia is installing fingerprint access systems at 500 branches to replace the password access system that they have currently. This is a large contract that has been awarded to a company called Fingerscan to implement and is worth approximately $8 million.

Biometrics is a lot more secure than a password, as Biometrics actually verifies that the person is who they say they are. For instance no fingerprint is identical, so if the persons fingerprint matches the fingerprint on record then the correct person has been authorized. With passwords this does not verify the person, it only verifies that the person has the correct knowledge i.e. the password. If somebody wants this information, then it is fairly easy for them to obtain it, as someone may tell them the information, they may see it written down somewhere, or they could just see someone typing it in. Of course to make an even more secure system, both Biometrics and passwords can be used together to create a two-layer security approach.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As well as Biometrics being more secure, they can also create cost savings in the long term. The reason that this is said, is that with a good password policy, the users have to have passwords which are complex and can easily be forgotten, which means that not only does it take the user longer to get into their computer to start work when the password has been forgotten, but they will also ring the Help Desk to have their password reset. The other advantage of Biometrics over passwords is that passwords need to be changed on a regular basis, whereas a Biometrics solution is for life. This means that instead of people having to spend time thinking of new passwords and involving the help desk with forgotten passwords, they can log straight into their computer or walk straight into the building to begin work.

In order to implement a Biometrics solution an infrastructure needs to be put in place. To gather the attributes required, you would need a device to collect the correct data, this would be a scanner for a fingerprint or a speaker for voice recognition. Once the data was collected it would need some specialized software in place to convert the attribute into a digital form. Within the system there would be a database that the attribute would be checked against using a specific algorithm to see if there is a match. If there was a match, then the identification is complete, and if no match is found, then the identification has failed. The Biometrics can be used individually, or several Biometrics could be used in one security solution depending on the level of security, which is needed.

In the diagram displayed below, you can see a sample authentication process.

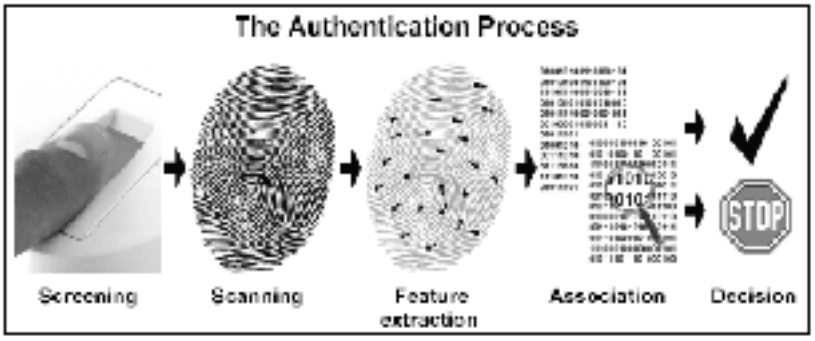


Figure 4: The Authentication Process [4]

IBM, Microsoft, Novell, and others are developing a standard, called BioAPI that will allow different manufacturers biometric software to interact with each other. As well as interaction problems, which are currently in place, there are also concerns regarding privacy issues with collecting and sharing Biometrics information. One solution to this problem that is being investigated is to encrypt the Biometric data as it is gathered and then erase the unencrypted data in order ensure privacy and eliminate identity theft.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Biometrics is very secure, as everyone does have unique traits, but there are of course limitations. The problem that we have currently is that although there have been huge developments in the area of Biometrics, the technology cannot be described as 100% accurate. There are products that are very accurate, but these are very expensive, and cannot be implemented quickly or easily and they still cannot be totally relied on. The other problem is that people may be able to fake Biometrics in order to get identification. This may sound like science fiction, but wasn't that what Biometrics technology implementations were described as a few years ago? In order to get round this problem, an implementation should include another layer of security such as a password or Smart Card and pin.

Biometrics is now coming of age and is being used in more and more industries. In 1990 the Biometrics market was just $6.6 million, but by 1999 the market was a staggering $63 million, and by 2004 the market is expected to have $500 million in sales according to the U.S National Biometrics Center. Manufacturers of these systems are looking into other areas where Biometrics can be introduced such as implementing Biometrics on a Smart Card, which will be discussed later in this paper.

Biometrics Implementations

Biometrics is now becoming used in various different industries and situations. During this section, I hope to give you an insight into the varied uses, which are in place today to give you an idea of the possibilities for the future.

The Dutch government is using iris-scanning techniques in Rotterdam as a trial to prevent identity fraud. The reason why they are looking into the use of Biometrics is because they have seen fraud by sharing the original documents increase. To start off with, they have scanned 250 people from ethnic minorities in Rotterdam who are waiting to see if they can stay in the country. While they are waiting for their applications to be processed, they have to report to the police once a month, and the Biometrics have been put in place to stop them from sending a similar looking friend or relative in their place. By 2003 the Dutch government has said that everyone that has a European Union Identity Card will have Biometric information stored on the card, and they are also looking to do this for passports as well, although a date has not been set for this. For these implementations, the Biometric data will not be stored on a database; it will only be stored on the card.

Biometrics is also used by Canadian Customs in order to facilitate the smooth transfer of goods across the border. To help truck drivers cross the border more quickly, they have their fingerprints registered and these are verified when they cross.

© SANS Institute 2000 - 2002, Author retains full rights.

In prisons within the United States, the hand geometry of the prisoners, staff and visitors are used to verify where they are within the prison. The details of their hand geometry are stored in a database, and they are issued with a swipe card, which must be carried at all times. Different levels of access control are issued to different areas within the prison. For example a member of staff would need to be given a higher level of access than a prisoner, so that they could gain entry to more areas of the prison.

In the United Kingdom LloydsTSB have been using Biometrics solutions with some of its customers, by inviting them to have their photograph placed on their credit card. This is so that when making purchases with their credit card, the persons' identity can be verified against the photograph.

Biometrics is even being used at places such as Disney World, where they use hand verification. This Biometrics solution is used to stop people from sharing their season tickets for the parks.

At present the most used form of Biometrics is the fingerprint, but this could all change as new solutions are developed and released making it easier and cheaper to implement solutions using different Biometrics.

As the need for Biometrics solutions intensifies, and the market develops, then the price of Biometrics solutions will be forced down, and we will witness Biometrics being implemented in more varied uses and more industries than ever before.

Using Biometrics and Smart Cards Together

Implementing Biometrics on a Smart Card is a very new technology. The reason why more new developments are coming about now is due to the fact that the memory capacity in modern Smart Cards has increased to make this a viable option.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As you can see below, putting Biometrics on a Smart Card uses a lot of space, which could be used for other storage.

Biometric	Bytes Required
Finger Scan	300-1200
Finger Geometry	14
Hand Geometry	9
Iris Recognition	512
Voice Verification	1500
Face Recognition	500-1000
Signature Verification	500-1000
Retina Recognition	96

Figure 5: Biometric Memory Usage [7]

Biometrics can be used in a variety of ways on a Smart Card. They can be used to protect the information that is actually on the card; in this instance the Biometric would be used to verify that the person trying to access the data is really the person whose data is stored on the card. Another reason for storing the Biometrics on the card could be to identify the person to a computer, so they'd verify that the Biometric on the card is that of the person trying to access the computer system. Biometrics could be stored on a Smart Card to be used as a passport, which would make it a lot more difficult for people to forge passports or to try and use someone else's passport. So as you can see, Smart Cards and Biometrics can work together to bring an even better security solution.

One of the main advantages of using Smart Cards with Biometrics is speed. This is because if you were implementing a Biometrics solution without a Smart Card, then the persons' attributes would have to be stored on a central database, which would take a lot of time to search, access and maintain. When using a Smart Card, the Biometrics data is stored on the card, so no time is wasted in searching a large database for the correct match. Another advantage of using Biometrics with Smart Cards is that if someone was to lose their Smart Card or have it stolen and it did not have a Biometric installed on the card, then someone could essentially take on the identity of that person. The idea of stealing someone's identity sounds a little dramatic, but this is happening more and more and people are not realizing that this has happened to them until it is too late and someone has either run up a lot of debt for them or even worse got them a criminal record. It is easy for someone to do this at present, but with using Smart Cards and Biometrics together, this could become a thing of the past or at least make it more difficult for the people who try to do this. As stated earlier, you could also have a Pin Number installed on the card to provide a second layer of security and make the infrastructure even more secure.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The future is bright for Smart Cards and Biometrics as more organizations show interest in using these separate technologies together. At the moment a lot of organizations cannot afford this technology, as it really is still in its developing stages, but as businesses demand more from their Biometrics and Smart Card solutions, the price will inevitably be forced down as new advances in technology are brought to the fore.

Smart Card & Biometrics Implementations

Although implementing Biometrics on Smart Cards is a very new technology, there are some implementations already in place, and there are a lot of industries looking into the technology. Since the terrible tragedy of September 11th the Airline industry and governments have been especially interested in this area of security.

The National Identity Card of Malaysia uses both Biometrics and Smart Cards. The Smart Card has both the persons' fingerprint and photo stored on the card. Later this year, new Smart Cards are going to be distributed with even more storage capacity. At present the cards, which are being issued, have 32kilobytes of memory, but the new cards are going to have 64kilobytes. At present there are several uses for the Smart Card that can be applied for. These are identity card, driving license, passport, personal health record, electronic cash, Touch 'n' Go payment card, and ATM card. However the Malaysian government is looking at even more applications for the cards. This is an area where we are going to see strong growth within the Biometrics and Smart Card industry. National identity cards are used within a lot of countries around the world, and a lot of countries are also looking to put an identification scheme in place. The Smart solution would be to use Biometrics and Smart Cards for a truly secure up to date implementation.

In the U.K, Asylum Seekers are given a Smart Card that has their fingerprint installed on it in order to stop forgery. Previously the Asylum Seekers were given a letter from the Home Office which contained details about them staying within the UK until their case was considered. The problem with the letter was that they could easily be forged, so this is why the Home Office has begun to distribute Biometric Smart Cards.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The financial industry is also looking into the use of Biometrics and Smart Cards by using them as an ATM Card. With the amount of financial fraud that is taking place in the world today all banks are looking into how they can make their systems more secure and they are saying that Biometrics and Smart Cards may be the answer. The easiest way in which they could use Biometrics would be to put a fingerprint on the Smart Card and have a fingerprint scanner at the ATM. However at a place called Swindon in the UK, the Nationwide Building Society is conducting a trial whereby when you try and get money out of an ATM your iris is scanned. It takes approximately 2 seconds for the iris scan to take place and then if identification is successful you can use the system as normal.

A lot of Airlines are using Biometrics and Smart Cards to conduct a trial for frequent flyers. The way in which they are doing this is to take a scan of the passengers' finger and then their finger is scanned once more as they go through the departure gate. This allows them to bypass some of the more stringent security checks on boarding.

There are a lot of organizations looking into ways in which they can implement this technology as they realize that it is not only secure, but it is truly scalable from a small organization to a truly global solution.

Conclusion

This document illustrated that a Smart Card is:

- A plastic card similar in size to a credit card that has a computer chip and a printed circuit embedded within it.

It also explained that a Biometric is:

- A physical attribute or behavioral characteristic of a person which can be used for authentication or verification

These technologies can be used either separately or together to provide a reliable security solution. When they are used together they are even more secure, as they can provide a multiple layer security solution. The other advantage of using them together is speed and the fact that the solution can be a small implementation or a worldwide solution.

Although there is a large initial outlay to have these solutions installed, the benefits that you gain from them can be immeasurable. In business today, if a security breach occurs, then customers can lose faith and move to another organization for their products or services, but if you have a good security solution installed such as Biometric Smart Cards, then it can mean the difference between keeping a large satisfied client base and going out of business.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. Chan, Siu-cheung Charles. “An Overview of Smart Card Security” http://home.hkstar.com/~alanchan/papers/smartCardSecurity/ (25/08/02)

2. “Definition Of Biometrics” http://stat.tamu.edu/Biometrics/ (26/08/02)

3. O’Sullivan, Orla. “Biometrics Comes to Life.” http://www.banking.com/aba/cover_0197.htm (26/08/02)

4. “Biometrics 101” http://www.biometricsdirect.com/Web/Biometrics/Biometrics_101.htm (27/08/02)

5. “Types Of Chip Cards” http://www.smartcardbasics.com/typesofchips.html (27/08/02)

6. Meloan, Steven. “Blue From American Express” http://java.sun.com/features/2001/05/amex.html?frontpage-banner (27/08/02)

7. Smart Card Alliance. “Secure Personal Identification Systems” http://egov.gov/smartgov/information/secure_id_presentation-v6-012802/sld011.htm (27/08/02)

8. Rash, Wayne. ”Biometrics Not A Sure Thing” http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2828675,00.html (28/08/02)

9. Travis, Alan. “Asylum Seekers to be given ID Cards” http://society.guardian.co.uk/asylumseekers/story/0,7991,583362,00.html (28/08/02)

10. Onley, Dawn. “DOD Double-Times Smart Card Use” http://www.gcn.com/vol1_no1/daily-updates/18719-1.html (29/08/02)

11. “Standards” http://www.smartcardbasics.com/standards.html (04/02/02)

© SANS Institute 2000 - 2002, Author retains full rights.