

Contents

1	Introduction to biometrics	2
1.1	“What you have or know” vs. “What you are”	2
1.2	Different biometrics, market share and efficiency	3
1.2.1	Fingerprint	3
1.2.2	Hand geometry	3
1.2.3	Iris	4
1.2.4	Others	4
2	Benefits and applications of biometrics for prisons	5
2.1	The users of the system	5
2.1.1	Inmates	5
2.1.2	Wardens	6
2.1.3	Visitors	6
2.2	Existing biometric security systems for prisons	6
2.2.1	Fingerprint-based systems	6
2.2.2	Iris, hand geometry and retina-based systems	7
3	Evaluation of an emerging technology for prisons	8
3.1	Are biometrics unbreakable ?	8
3.1.1	Face recognition	10
3.1.2	Fingerprints	10
3.1.3	Iris	11
3.2	Privacy vs. security	12
3.3	Does it really solves the problems of traditional systems ?	13
3.3.1	Does it suffer of conceptual flaws ?	13
3.3.2	Answer to some assumptions	13
3.3.3	Different scenarios	14
3.4	Conclusion	15

Chapter 1

Introduction to biometrics

1.1 “What you have or know” vs. “What you are”

Traditional approaches to secure access are based on “what you have” (tokens), “what you know” (passwords, PINs) or both. These methods bring with them their collection of issues. Tokens can be lost or stolen while passwords may be forgotten by users, reused for different applications or even written down.

Recognition of the above does not mean identification of the person presenting it. The reason being that anybody in possession of your tokens or having knowledge of your PINs or password may provide them too.

Biometric technologies tend to address the problems of the traditional approaches by using biological traits or behavioural characteristics to identify an individual.

As for validating an individual’s identity, there is a distinction between verification and identification. The first, verification, resolves the question “Am I who I claim to be ?” by denying or confirming the claimed identity. The second, identification, involves establishing an individual’s identity, therefore answering to the question “Who am I ?”.

Among the features used to achieve identification and verification are fingerprints, hand geometry, iris, face and voice. No two individuals are alike. Therefore, by being irrevocably tied to the individual, biometrics is obviously well placed to address the issues of traditional approaches.

However, biometric security systems all come with their advantages and shortcomings. Like most new and innovative technologies, biometric security systems suffer of weaknesses in terms of effectivity, reliability, convenience and efficiency. Therefore the key to assess security systems with efficiency is to gain a deeper insight into the relevant aspects of biometrics by embracing both the experiences of the past and the latest research findings and developments.

After briefly presenting what biometrics is and what we shall expect of it, in term of security and advantages, over the traditional systems, this report will focus on current features and weaknesses of biometrics. Finally, the level of fulfillment of the requirements and an analyse of the remaining problems will give a clear and deep insight on the current status biometrics and give conclusion as for its use in Guernsey Prison.

1.2 Different biometrics, market share and efficiency

1.2.1 Fingerprint

With 36%¹ of the market share, fingerprint recognition has been around the longest and is currently the most accepted biometric in use for authentication systems. A lot of research is carried out and many applications have been deployed. It is well accepted by users and is quite 'effortless'.

Fingerprints recognition is however suffering of a high false rejection rate (FRR). It requires high-quality image for enrollment, which might be very expensive. Injuries to fingers as well dirt and moisture may affect successful recognition.

1.2.2 Hand geometry

Hand geometry, with 27% of the market, is not far behind fingerprints recognition. Unlike fingerprints, the human hand isn't unique and, because the features are not descriptive enough, it can therefore not be used for identification. However, hand geometry is surprisingly accurate for recognition. A very robust verification can be obtained by combining hand geometry with another biometric.

¹The given market shares have been obtained from an interview with John Chang from Allied Business Intelligence. [findBiometrics, 2003]

1.2.3 Iris

If iris recognition is currently hitting only 16% of the market, it is one of the fastest growing areas of biometric technology. It is by taking advantage of the extraordinary amount of detail in the pigmented membrane surrounding the pupil that iris recognition is the most accurate biometric identifier. If iris recognition is currently the most accurate biometric, it is also the one that is the least accepted by users who fear their eyes to be damaged by iris scanners and therefore public acceptance remains the main concern.

1.2.4 Others

As for retina scan (11% of the market shares), the patterns of the blood vessels in the back of the eye are measured. Retina scan used to be the most accurate biometric but is most likely to become obsolete because it is not well accepted by users and is now less accurate than iris.[Retina Scan Technology, 2003] Known as the biometric that would detect terrorists in a crowd, the face recognition has suffered of a bad reputation in terms of privacy and efficiency. New technologies involving the three-dimensional analyse of the face are getting over this former reputation. Voice recognition or speaker recognition, with the speech signal allows to perform both identification and verification.

Chapter 2

Benefits and applications of biometrics for prisons

2.1 The users of the system

2.1.1 Inmates

As far as the inmates are concerned, the implementation of biometrics security systems in prisons can be aimed at two major tasks.

The first one is to give them access the the different facilities. This can be automatically based on differents criteria such as current time of the day or their own “profile” of permissions to access some facilities. For example, only the inmates in charge of a specific service would be allowed to access the facility of that specific service and only during the time slot allocated for that purpose.

The second and even more critical task is to handle the releases of inmates. Impersonating an inmate that is to be released is a potential way to escape from a prison. If the inmates are recognised with the picture on their file, it may well happen that a human error would lead to the release of the wrong person. But if the verification is carried out with the use of biometrics, since the inmates are identified thanks to their own and unique characteristics, that kind of attempt would be directly defeated.

In terms of accountability, the use of a biometric security systems offers an automated way to verify in real time that no inmate is missing but also to monitor their movements. For example, if an inmate has not been through the access control at the canteen for lunch, it is possible to automatically

trigger an alert message to the staff with accurate information such as where the missing prisoner has been checked by the system for the last times.

2.1.2 Wardens

For the wardens, the use of biometrics, as a replacement to the traditional means, is an obvious improvement regarding three major concerns.

First of all, the management of the keys is a major issue. They have to be collected, through secure means, before the duty and given back afterwards. The loss of a key compromises the security of the prison and requires all the relevant locks to be replaced. Such a replacement is not only very expensive, but also a potential security risk. Then comes the problem of the PINs to remember, as they are often changed. Finally, while they are in contact with the inmates, because they are carrying the “ways to escape the prison”, the wardens become a target and this affects their own safety.

Also, because the wardens are the only one accessing the most restricted areas, a biometrics security system would allow a secure verification of their identity before granting them access to the prison.

2.1.3 Visitors

Even if the visitors are only granted access to a restricted area, the control of the flow generated by them is an important point. The visitor, at their first visit, are required to fill forms. Then, at each following visit, they have to make proof of their identity. A biometric system would permit, after an enrollment of the visitors, to both make sure that the visitor is already know but also to only grant him access if a meeting has previously been set.

2.2 Existing biometric security systems for prisons

2.2.1 Fingerprint-based systems

Identix has implemented two security systems for prisons. [Engler, 2001] The first solution is featuring the Fingerscan V20 and a mag-stripe card. Every inmate is given one of this cards which embeds his fingerprint and is his identifier. For accessing the different facilities, ownership of the card being slided in the mag-stripe is verified afterwards by scanning the finger of

the inmate and checking its match with the one embedded in the card. The second solution is featuring the DFR90 reader (now replaced by the DFR2090) [DFR2090, 2003] and the Bioengine SDK [BioEngine SDK, 2003] to capture and store the fingerprints. In this case, the inmates do not need to use a card anymore because they are identified with their fingerprint.

Smith Heimann Biometrics has implemented access control in German prisons using different fingerprints scanners such as ACCO 1394 and LS2 CHECK that have been “customized to prison’s needs”. [Appendice A] The German company CI2T provides a biometrics security system. They have developed the applications to handle a CCD sensor supplied by Delsy AG. In prisons, the system is not used by the staff but by the inmates only. Their system is running since April 2000 and the company says that the users acceptance was good. When asked how the biometrics data were stored and protected, it has been answered that they were saved on a server which is protected from the Internet by a firewall.

2.2.2 Iris, hand geometry and retina-based systems

Like Identix, Iridian is a leader in the implementation of biometrics-based security systems for prisons. They started in 1996 and already have their systems installed on 30 county prisons and 10 states prisons. Using iris scanners, their systems can achieve identification of the inmates. This system has proved to be very efficient especially at defeating attempts from prisoners to impersonate inmates to be released. [Appendice B]

Recognition System has developed a biometric security system based on the hand geometry. [Recognition Systems, 2002] The system is essentially used by the staff and is not aimed at being used for controlling access of the inmates to the different facilities but most likely to avoid the use of keys and their related problems.

Some of the county jails in Utah and Florida are already running retina scanners sold by Eyedentify. [Beiser, 1999] “Eyedentify went out of business [...] When it was first introduced, Eyedentify offered one of the highest reliability rates around, 1:4000, better than any other biometric. No face available, hand geometry was 1:400, fingerprints took a long time and had a high error rate. Since then, fingerprint error rates have improve. 1:10,000, and iris recognition has come along to blow them out of the water with an error rate of 1:1.2 million! They could not compete and could not change the product enough to recapture market space.” [Appendice B]

Chapter 3

Evaluation of an emerging technology for prisons

The critical problems raised by the use of traditional security systems involving tokens and PINs have already been clearly defined. At first sight, it also appears that biometrics, by not only addressing current problems, but by also bringing more advantages, is the only technology able to guarantee systems to be even more secure, efficient, accurate and effective.

Over the past years, emerging technologies have not always been able to deliver what they promised. Biometrics makes not exception to this rule. Therefore, having a very critical approach is the only reasonable way to assess and confirm whether or not such a technology can cope with the security requirements of a prison.

Furthermore, as biometrics is a technology that deeply deals with people's identity, serious concerns are being raised over an often neglected issue: the privacy. While the security remains the main concern in the correctional environment, it also remains mandatory to make absolutely sure that any collected data can not be misused.

3.1 Are biometrics unbreakable ?

Most of the studies on biometrics are evaluating the efficiency of different systems with regards to their False Rejection Rate (FRR) and False Acceptation Rate (FAR). A False Rejection happens when an enrolled user is not recognized by the system and is therefore not granted access. On the other

hand, a False Acceptance is the event of a user whose biometric features are not registered in the system to be granted access.

Since these studies and figures are generally carried out and published by the vendors themselves, it is hard to believe that being utmost critical with their own products is their main concern. It is also hard to believe that they would publish any bad results. In 2001, the Darmstaedter Fraunhofer-Institut, in collaboration with the BSI (German Federal Institute for IT Security) conducted series of tests on different biometrics systems that were given by vendors. Obviously because of pressure from the vendors, the results of this independent test were never published.

As a conclusion to this matter of facts, the vendors are certainly the last one to trust when evaluating systems. Therefore, the only way to have a system assessed is let an independent organisation trying to break it by any ways.

Lisa Thalheim, Jan Krissler and Peter-Michael Ziegler have conducted series of tests on eleven biometrics systems, in November 2002's issue of the German magazine *c't*. [C'T, 2002] They describe three different approaches to break a biometrics system.

The first approach entails tricking the system with artificially created data. A good example is the creation of an artificial fingerprint from traces left on a scanner. This approach involves the ability to get the relevant biometric data.

The second way is the so-called replay attack. In this scenario, while a user is being checked for his identity by the system, the data sent by the scanner over the wire that connects it to the system are collected. This data can then be sent over the wire again, to replay the authentication and get access granted.

The last approach consists of attacking the database storing the biometric data. In this case, the attacker would for example add a user with his fingerprints pattern in the database and grant to that user access to restricted areas.

3.1.1 Face recognition

Cognitec's Face VACS-Logon features face recognition working with the aid of a webcam. The testers from the c't magazine have proceeded in different stages for testing this recognition system.

When a user enrolls in the system with the VACS-Logon, a serie of pictures is taken and stored on the system. This pictures are neither encrypted or protected in any way. Therefore, they started by taking this freely-available pictures from the computer and to display them on the screen of a laptop which would then be presented to the system. After having tried different distances between the screen and the webcam, the system finally granted access.

Since accessing the system to get the pictures of authorized users is not always feasible, they then took three pictures of a user in different lighting conditions, as if the pictures had been taken secretly. The second picture showed to the webcam unlocked the protection system sucessfully.

Cognitec has integrated a higher level of security called Live-Check that can be enabled to prevent deceptions with pictures. Once enabled, if the previous attacks did not work anymore, the system also suffered of having the users hardly recognized at first try. They then made a movie of an authorized user to be then shown to the webcam with the aid of a laptop. Once again, after the right distance had been found, access was again granted.

3.1.2 Fingerprints

If the features of the fingers is what most of the products are currently relying on, this is also the recognition mean that has produced most of the stories on how biometric systems can be defeated.

After biometrics vendors have claimed for many years that the products they sell are highly secure and impossible to fool, some doubts were shed after Tsutomu Matsumoto, a Japanese cryptographer from Yokohama National University defeated systems with the use of cheap, easily obtainable materials and tools such as the gelatin that gummies are made of. In a very comprehensive report [Matsumoto, 2002], he explains how he proceeded to create the fake fingers that he then used to sucessfully defeat eleven of the fifteen readers that he tried to attack. By putting a life finger in a plastic-mould and then filling it with gelatin, he was able to fake a finger able to

defeat systems 80% of the time.

In a real life scenario, it would be difficult to secretly acquire fingerprints in a such way. As an answer to this matter of fact, Tsutomu Matsumoto created a second finger by enhancing the image of a latent fingerprint left on a glass. The image was printed and applied to a photo-sensitive printed-circuit board which allowed to create a three dimensional mould in which the gelatin was poured. This second fake finger also achieved to defeat scanners 80% of the time. Besides the computer and printer for processing and printing the image, all the other required material were very cheap and easy to obtain from groceries and electronic stores.

By using similar techniques but different material such as wax, silicon or just a thin-walled water-filled plastic bag, the team of the German *c't* magazine has been able to defeat all of the eleven different systems they were testing. A report from Ton van der Putte shows how, with the aid of a silicone rubber moistened with saliva, he has also been able to defeat different fingerprint scanners. [Putte, 2000] In the November 2003's issue of *Crypto-Gram*, he gives an update on his achievements and reports to have tested his dummy fingers again and to have been able to recently fool sensors from about 20 brands. [Crypto-Gram, 2003] This series of successful attacks tends to confirm the fact that fingerprint-based security system can be quite easily bypassed.

Recent fingerprint scanners should address such weaknesses with the aid of sophisticated "life checks" measuring pulse, heat and perspiration. Starbug and Lisa, two German hackers recently performed similar attacks as Tsutomu Matsumoto, during the Chaos Computer Camp 2003, an annual meeting of hackers given every summer in Berlin. [Security Focus, 2003] Using latex, instead of gelatin they have been able to create fake fingerprints too. "This life checks might be defeated too, if the material is thin enough to possibly allow the information to pass through", said Starbug. This last scenario presents an even more credible threat.

3.1.3 Iris

However iris recognition is said to be the most secure biometric, the team of *c't* magazine has been able to defeat during their tests the only one iris scanner they had been given: a Panasonic's Authenticam BM-ET100. To sum up the results of their investigation, it has been found that presenting

to the scanner the image of an iris printed on a sheet of paper would not defeat the system. Reason being that a “life check” verifies that the pupil is alive. Since the pupil is not being checked for identity, they had the idea to cut, in the middle of the image, a small hole behind which the pupil of an actual human being would be hidden. Here again, the system granted access.

3.2 Privacy vs. security

Demonstrated in several scenarios, the misuse of collected data has made the general public aware of the fact that Big Brother might be watching. On the other hand, while the security is also a critical issue, having to make a choice between privacy and security leads to an impasse. The International Biometric Industry Association (IBIA) has published a list of Privacy Principles [IBIA, 2003] that are aimed at are guiding the vendors into a respect of the privacy. Further more, to avoid critics about the privacy issues that may occur with the misuse of biometric data, telling the truth is the key to credibility.

Because, only a part of the public really cares about the privacy, the policies are often not respected and data misused. In the correctional environment, a huge amount of data are gathered about the inmates. Since this collected data may be precious for the sake of national security, the general public would certainly not mind to have them propagated between different services.

On the other side, data gathered by the logs of biometrics systems allow to know in real-time the location of each inmate, to tell exactly at what they accessed different facilities. For security reasons, it is required to keep this logs that would be used in case of an escape. However, keeping such information for a period longer than 24 hours seems to not be useful anymore and therefore, as part of respecting the privacy of inmates, such information should not be kept.

3.3 Does it really solves the problems of traditional systems ?

3.3.1 Does it suffer of conceptual flaws ?

It has been clearly demonstrated that the first weakness of the biometrics is that it is fairly easy, furthermore with just simple means, to steal the identity of someone and to then reproduce it for an impersonation.

Philippe Wolf is the director of the DCSSI, the governmental agency in charge of dealing with IT Security questions in France and working in collaboration with the Defense Ministry. In October 2003' issue of *Infosecu*¹, he explains why the use of biometrics should not be recommended. [Infosecu, 2003] His first argument is the already explained problem of the easiness to achieve an impersonation attack. The second argument raises another critical problem of biometrics: when a PIN, a password or a token is compromised, the rule is to replace it. The fact that this is not possible with biometrics has for consequence that, once compromised, an iris, for example, can not be used for identification anymore. He gives as an example, a scene in the movie "Minority Report" where the hero's iris is "black listed" and he is required to have a chirurgical intervention to have a new one.

3.3.2 Answer to some assumptions

Like any system, biometrics has weaknesses and it is now important to see wheter or not the assumptions made about it are still true. With the information given so far, the following answers can be given:

- *"Biometrics is the only one system that can proof that you are who you claim to be."* Since systems have been so easily defeated, this is false.
- *"Biometrics, unlike tokens and PINs, can not be stolen."* Yes they can and, furthermore, without its owner to even notice it.
- *"With biometrics, you are your key"* Yes, a key that can still be compromised and can't even be replaced.
- *"Multimodal biometrics makes it even harder to defeat a system"* If different biometrics have been independently defeated, once gathered they remain as much attackable.

¹Infosecu is a magazine published every month by the Centre National pour la Recherche Scientifique (CNRS)

- *“If a security officer verifies that the biometric used is alive, the use of fake fingers, iris, face and others can be avoided.”* Not definitely. If simple attacks have been so successful, more advanced ones involving more efforts to hide the fake fingerprint, iris, face, voice or hand should be able to cope with a security officer’s check.
- *“With biometrics, identification and authentication can be automatically achieved.”* If the presence of a security officer is still required to validate the use of the system, then this is not fully automated.
- *“Biometric are running in different prisons and have defeated escape attempts.”* This does not mean that the systems are secure and even if they are, a security flaw might still be discovered.
- *“False Acceptance Rates are the representation of the systems level of security.”* Most of the systems defeated in the past claimed FAR as low as 0,0001%
- *“Replacing the lock in a prison, after a key has been compromised, is extremeley expensive.”* This is obviously right but certainly the impact of a compromised biometric is not cheap either

3.3.3 Different scenarios

Once identified, the weaknesses of biometrics allow to guess some possible scenarios:

Joe is to be released by next month. Aware of this, Bob offers him a glass of water. To remember Joe’s face after he will have been freed, Bob uses his new high resolution digital camera to take close and distant pictures of Joe and also to record a small movie of him talking. By doing this, Bob has been able to steal Joe’s fingerprint, face, iris and voice. Providing this digital information by mail to a Alice, his wife, he will wait for her to produce the relevant fakes that she will discreetly give him at her next visit. In the morning of Joe’s release day, Bob will pop up at reception and use the fakes to bypass the biometric systems. The same scenario can be applied with a warden as the victim of Bob.

To ease remote administration and maintenance, the company that installed the biometric system in the prison has connected it to the Internet. To ensure that the system won’t be attacked, they have protected it with a secure firewall. Alice is aware of a recent security flaw found to defeat

firewall protections. She tries to attack the system and is successful because the vendor has not yet applied the security patch that addresses this flaw. She updates Bob's entry in the database to grant him the permission given to the wardens and calls Bob to tell him. Bob then attacks a warden to steal his clothes and leaves the prison, as a member of a staff would do.

This scenarios, that would well have their place in a Hollywood movies, are in fact potentially possible. If cheap, easy to obtain materials have allowed to defeat so many systems, the use of more sophisticated techniques should allow this scenario to happen.

3.4 Conclusion

Prisons are characterised by a *"rapid population turnover and provide frequent access to a variety of official and nonofficial visitors."* [Turner, 2000] The deluge of PINs and keys to handle, the risk for them to be compromised and the need of real-time accountability are just a few of the challenges that a prison manager has to face.

These major security concerns are the reason why the correctional facilities have become a huge market for biometrics vendors. Based on the features of the human beings - what you are - instead of what you have or know, the implementation of biometrics systems promises to not only wipe out all the current weaknesses of the traditional systems but also to bring additional advantages such as guaranteeing the identity.

Emerging technologies have often proved to promise more than they could deliver. Over the past years, several attacks defeating different biometrics systems have demonstrated that this matter of fact also applies to biometrics. This deceptions have not only proved that most systems were weak but also that a compromised biometric can not be replaced like a token or a PIN. This may give a new definition to biometrics:

"You are your key. A key that can be compromised. A key that can not be replaced."

To increase the strength of biometrics systems, the tendance is to add even more control means, like adding passwords and tokens to the authentication or to limit the perimeter of its use. Built on top of the traditional system, biometrics may bring more security. However, an addition to the traditional system is not what is expected from a technology meant to re-

place it. Furthermore in addition to keep the already existing disadvantages of the traditional system, this would furthermore bring the disadvantages of biometrics such as the false rejection and make the system significantly less convenient.

Biometrics recognition systems, like any layered systems, have the strength of their weakest links. A reader may well be almost impossible to break, if the database containing the information has a weak security protection, the system remains easy to defeat.

Biometrics is an empirical science which is a constant challenge between the developers of systems and their attackers. While this allows to reveal shaming weaknesses of vendor's current implementations of biometrics, this process of evaluation and assessment is also the key to the improvement in any security systems. A good example of this is the cryptography. After centuries of codes improvement and code breaking, cryptographers have now achieved with the use of the so-called Public Key Infrastructure, a level of strength that can't be broken within a human life.

Biometrics was not discovered very recently but has been around and actively used for many decades. Systems are getting more accurate, especially at detecting features of the body to be alive and thus avoiding attacks using fake features.

People claiming their systems to be impossible to break must never be believed because the assumption that, not any system is ever totally secure, has been proved several time. Any security system is empiric and can well be said highly secure for many years and be defeated tomorrow. This does not either mean that the use of security system is pointless. This however points out the fact that a really secure environment involves both the use of systems that have proved a high level of strength against attacks and the awareness that system remain secure only as long as no exploitable weakness has been found.

Since the strengths biometrics security systems still have a short lifecycle and therefore still suffer of both technical and conceptual weaknesses, they have not yet proved to deliver what they promised. Therefore, as the level of security of Guernsey Prison is a main concern for public safety, the use of biometrics is certainly not to be recommended yet.

Bibliography

- [findBiometrics, 2003] Feature Reports, Biometrics Industry Report: An Interview with John Chang. Retrieved November 1, 2003, from http://www.findbiometrics.com/Pages/feature\%20articles/john_chang.html
- [Retina Scan Technology, 2003] International Biometrics Group. Retrieved November 1, 2003, from http://www.retina-scan.com/retina_scan_technology.htm
- [Engler, 2001] NLETC, 2002, October 4, News Summary. Retrieved November 1, 2003, from <http://www.mail-archive.com/justnetnews@nlectc.org/msg00081.html>
- [DFR2090, 2003] Identix web site, Products, Single fingerprint readers, DFR 2090. Retrieved November 5, 2003, from http://www.identix.com/products/pro_ls_desktop_dfr2090.html
- [BioEngine SDK, 2003] Identix web site, Products, Platforms and SDKs, BioEngine SDK. Retrieved November 5, 2003, from http://www.identix.com/products/pro_sdks_bioengine.html
- [Recognition Systems, 2002] Recognition Systems web site, Case Studie #12, Northern Ireland Prison Service. Retrieved November 5, 2003, from <http://www.recogsys.com/news/casestudies/cs12.htm>
- [Beiser, 1999] Beiser Vince, Wired News, 1999, August 21, Biometrics Break Into Prisons. Retrieved November 2, 2003, from <http://www.wired.com/news/technology/0,1282,21362,00.html>
- [C'T, 2002] Thalheim Lisa, Krissler Jan, Ziegler Peter-Michael, c't Magazine, November, 2002, August 21, Koerperkontrolle, Biometrische Zugangssicherungen auf die Probe gestellt, p. 114. Retrieved November 9, 2003, from <http://www.heise.de/ct/02/11/114/>

- [Matsumoto, 2002] Tsutomu Matsumoto, 2002, October, Importance of Open Discussion on Adversial Analyses for Mobile Security Technologies, A Case Study for Identification, International Biometrics Group. Retrieved November 9, 2003, from <http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf>
- [Putte, 2000] Ton van der Putte, 2000, September 21, Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, Esire, an Origin Extended Enterprise. Retrieved November 14, 2003, from <http://cryptome.org/fake-prints.htm>
- [Crypto-Gram, 2003] Ton van der Putte, 2003, November 15, Hacking Fingerprint Readers, Crypto-Grams. Retrieved November 16, 2003, from <http://www.schneier.com/crypto-gram-0311.html#9>
- [Security Focus, 2003] Harrison Ann, 2003, August 13, Hackers Claim New Fingerprint Biometric Attack, Security Focus. Retrieved August 14, 2003, from <http://www.securityfocus.com/news/6717>
- [Infosecu, 2003] Wolf Philippe, 2003, October, De l'authentification biometrique, Securite Informatique, Numero 46.
- [Turner, 2000] ITurner Allan, 2000, October, Applying an Emering Technology to Jails, American Correctional Association, Vol 62, No. 6
- [IBIA, 2003] IBIA, 2003, November 06, Privacy Principles. Retrieved November 16, 2003, from <http://www.ibia.org/princip1.htm>