Information Security Journal: A Global Perspective
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uiss20

Choosing a Biometric for Nonrepudiation

Panagiota Lagou [a] & Gregory Chondrokoukis [b]
[a] Economic University of Peiraeus , Athens, Greece
[b] Economic University of Peiraeus, Technology Education and Digital Systems , Athens, Greece
Published online: 08 Feb 2011.

To cite this article: Panagiota Lagou & Gregory Chondrokoukis (2011) Choosing a Biometric for Nonrepudiation, Information Security Journal: A Global Perspective, 20:1, 17-24, DOI: 10.1080/19393555.2010.544700

To link to this article: http://dx.doi.org/10.1080/19393555.2010.544700

Information Security Journal: A Global Perspective, 20:17–24, 2011

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2010.544700

Taylor & Francis
Taylor & Francis Group

Choosing a Biometric for Nonrepudiation

Panagiota Lagou[1] and Gregory Chondrokoukis[2]
[1]Economic University of Peiraeus, Athens, Greece
[2]Economic University of Peiraeus, Technology Education and Digital Systems, Athens, Greece

ABSTRACT Nonrepudiation is currently legally supported by digital signatures. However, problems with digital signatures have been analyzed in several papers, which consequently create doubts for the signatures' ability to support nonrepudiation. The addressing of weaknesses of digital signatures through the use of biometrics has also been considered. The scope of this paper is the identification of the most suitable biometric technology to be used for nonrepudiation purposes.

KEYWORDS information security and risk management, access control, application security, biometrics, nonrepudiation

DEFINITIONS

Some important principles required for the comprehension of this article are defined as:

1. **Nonrepudiation:** The principle that provides protection against false denial of having been involved in a communication (ISO, 1989).
2. **Biometrics:** A security identification system that measures a physical feature, such as hand geometry, retinal scanning, fingerprints, facial, or vocal feature; translates it into a digital form; and compares it with the values found in the approved database (ASIS, 2008).

OBJECTIVE

Nonrepudiation is currently legally supported by digital signatures (European Commission, 1999; European Commission, 2008). However, problems with digital signatures have been analyzed in several papers (Ellison & Schneier, 2000; Perez, 2000; Goulet, 2009; Adams & Just, 2007; Chondrokoukis & Lagou, 2009), which consequently create doubts for their ability to support nonrepudiation. The most significant problem that has not been solved is the protection of the private key. If protection of the private key cannot be enforced or verified in any way, nonrepudiation cannot be implemented. Solving of weaknesses of digital signatures through the use of biometrics has been considered (WP3, 2005; Kholmatov & Yanikoglu, 2006; Shan, 2009).

Address correspondence to Panagiota Lagou, Economic University of Peiraeus, Athens, Greece.
E-mail: panay_lang@yahoo.com

The scope of this paper is the identification of the most suitable biometric recognition technology for nonrepudiation purposes. Security of the chosen biometric is the requirement that will be evaluated. The reason security is considered is that it is a prerequisite for the provision of nonrepudiation. If the biometric recognition technology used in a transaction is not secure, which means unauthorized use can occur (either forged or stolen), then an entity can repudiate his/her participation in a transaction.

INTRODUCTION

Several biometric recognition technologies have been developed with varied usage and characteristics. The choice of a biometric recognition technology relates to the application/purpose for which it will be used. For the provision of nonrepudiation, an essential parameter is to prohibit the unauthorized use of the biometric in order to mitigate risk of a user denying participation in an electronic transaction. In order to choose the best biometric for implementing nonrepudiation, we define important characteristics and evaluate each biometric recognition technology with respect to those characteristics.

Nonrepudiation: Digital Signatures Versus Biometrics

According to European Directive 1999/93/EC (1999), in order for nonrepudiation to be implemented in electronic transactions, an "advanced electronic signature" should be used. An advanced electronic signature is an electronic signature which should meet the following requirements:

(a) It is uniquely linked to the signatory.
(b) It is capable of identifying the signatory.
(c) It is created using means that the signatory can maintain under his sole control.

Requirements (a), (b), and (c) are implemented by digital signatures through the use of the private key and through the assumption that it is verified that the private key is always under the user's possession. The most significant problem is that the protection of the private key cannot be ensured through the Public Key Infrastructure. In the case where the private key is compromised or the user disputes its sole possession, then nonrepudiation is not satisfied.

Biometric recognition technology satisfies the specific legal requirements. Since biometric data derive from the human entity, it can "be uniquely linked to the signatory," "is capable of identifying the signatory," and "is created using means that the signatory can maintain under his sole control" (European Commission 1999).

Additional advantages of biometric recognition technology in comparison to digital signatures, which facilitate the implementation of nonrepudiation, are (Lagou & Chondrokoukis, 2009):

- The use of biometrics is more user friendly than digital signatures. The user does not have to remember a secret code or hold a device where the digital signature is stored. The biometric can be provided whenever it is requested by the use of the relevant biometric reader.
- The digital certificate has a predefined life limit. This means that periodically the user should enroll again for a new certificate. The enrollment for a biometric takes place only once and can be used for a long period of time under normal conditions.
- The use of biometrics does not have any security requirements from the user side, which makes it easier to enforce nonrepudiation services.

Biometrics also have disadvantages, which can be solved. The most significant are (Lagou & Chondrokoukis, 2009):

- **Spoofing:** Spoofing is the representation of a false biometric claiming to be the legitimate one. This is the most significant weakness of biometrics. This attack can be defeated with methods such as "liveness" detection, which is used to verify that a live user has presented the biometric sample. Liveness detection methods have been presented in several papers as well as other protection methods.
- **False enrollment:** Good authentication and enrollment procedures are required. With the implementation of a secure infrastructure, this problem can be solved.
- **Reuse of provided biometric sample stored in the reader:** This threat can be defeated by the use of a reader, which does not store biometric data presented upon processing.

- **Biometric destruction:** If the biometric data used are destroyed (e.g., by an illness), this can create a problem with the authentication procedure (Schneier, 1999). This problem can be solved by the provision of an alternative biometric sample, which will be used in such cases.

At this point, it is important to note that we do not mean to reject digital signatures as a technological method for authentication or for many other applications in which they are useful and their operation has proven successful. Their ability regarding the implementation of nonrepudiation is their only operation under consideration.

MODEL DESCRIPTION

The recommended model is described in Figure 1. Steps that are shown in Figure 1 are:

1. The user contacts the public organization which supports the infrastructure for the provision of nonrepudiation through the use of biometrics and goes through the registration procedure, under which a biometric sample is recorded. The registration process should be conducted on the premises of the public organization, with the physical presence of the user and upon the demonstration and checking of identification documents such as ID card or passport in order to avoid impersonation. The biometric sample linked with the user identity is stored in a database. Strict security controls should be implemented to ensure protection of the biometric sample (e.g., database encryption, access control through the use of personal username-password, strict password policy, logging capability).
2. When the user wishes to take part in an identity verification procedure during an electronic transaction, he uses the biometric reader device. An image of his biometric characteristic is transmitted encrypted to the server of the second transacting party.
3. The second transacting party sends the image of the user's biometric characteristic along with the user credential to the public organization for identity authenticity verification.
4. The organization receives the biometric sample, decrypts it, and compares it to the one which is stored. If it matches, a positive reply is sent. If it does not match, a negative reply is sent.
5. The second transacting party has now verified the identity of the first transacting party and proceeds with the transaction (Lagou & Chondrokoukis, 2009; Lagou, 2010).

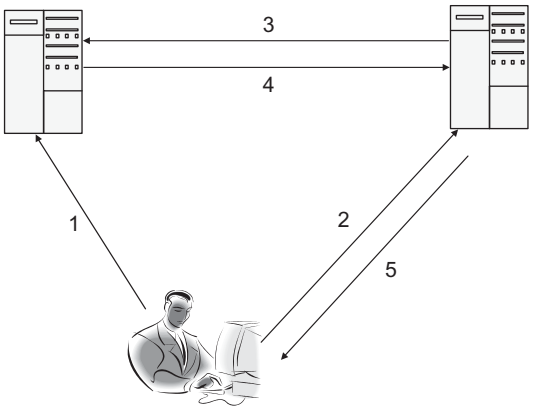

FIGURE 1 Nonrepudiation model through the use of biometrics.

FACTORS

The authors consider the following factors the most important for the choice of a biometric recognition technology for the viable implementation of the proposed model for nonrepudiation:

1. **False Acceptance Rate (FAR).** The most important factor is the possibility that an individual may present a biometric to impersonate another individual. Therefore, FAR should be as low as possible. If the biometric system suffers from false positives, users may be able to repudiate their participation in a transaction and consequently non repudiation cannot be implemented. That is why we consider this factor to be of high significance.
2. **False Rejection Rate (FRR).** This factor is the possibility of the biometric system not recognizing an authorized user and consequently denying access. This factor encumbers the process of provision of the biometric sample, but it does not violate nonrepudiation. Therefore, we consider it to be of medium importance for the provision of nonrepudiation.
3. **Resistance to forgery.** The biometric should be resistant to forgery. If forgery can take place, then nonrepudiation cannot be provided since the user can dispute his participation in a transaction. The

authors consider this factor to be of high significance as well.

4. **Resistance to environmental conditions.** The biometric technology may be used at any place. Therefore, it should be affected the least by external conditions such as light, dust, and noise. However, if environmental conditions are not appropriate to facilitate the provision of the biometric sample, this may hinder the process but does not violate the nonrepudiation principle. Since nonrepudiation is not violated but the process of provision of the biometric sample is hindered, we consider this factor of medium importance.
5. **Resistance to alteration.** It is important that the biometric used is resistant (as much as possible) to alteration through time or due to illness. In cases where the biometric is altered, it cannot be provided as authentication mechanism in a transaction. However, nonrepudiation is not breached, and therefore we consider this parameter of medium importance.
6. **User acceptance.** The user should be able to use the biometric with relative comfort. Even though this factor is important, we consider it to be of medium significance for current analysis since it hinders the process but cannot result in the repudiation of participation in a transaction.
7. **Cost.** Cost is an important factor concerning the implementation of a biometric system and its wide usage. However, it does not affect the implementation of nonrepudiation, nor does it create problems to the authentication process. That is why we consider it to be of low importance.

The evaluation of the above factors is defined in Table 1.

Factors were evaluated based on the following:

TABLE 1 **Factors' Evaluation**

Significance Factors	High	Medium	Low
FAR	√		
Resistance to Forgery	√		
FRR		√	
Resistance to External Conditions		√	
Resistance to Alteration		√	
User Acceptance		√	
Cost			√

- **High significance:** Without this factor, nonrepudiation is completely violated.
- **Medium significance:** The process of the provision of the biometric sample is hindered but the nonrepudiation principle is not violated.
- **Low significance:** The implementation of the process may be made more difficult, but neither the implementation of nonrepudiation nor the process of the provision of the biometric sample is affected.

This paper focuses on providing nonrepudiation in electronic transactions (the recommended model is described earlier). Factors used and relative weights would be different if different perspective was evaluated, such as commercial or privacy problems.

Factors' Analysis

For the selection of a biometric recognition technology, four biometric technologies will be compared which are more widely used:

1. Fingerprint
2. Iris
3. Face
4. Voice

Other biometric recognition technologies exist such as dynamic signature, keystroke dynamics, retina recognition, gait/body recognition, and facial thermography (NIST, 2006).

False Acceptance Rate – False Rejection Rate

In order to come to conclusions regarding factors FAR and FRR, the results from the test "Biometric Product Testing Final Report" (Mansfield, 2001) have been taken under consideration. Concerning the FAR, the results are:

- **Iris** has 0.0001% FAR with 2% FRR.
- **Fingerprint** has 0.0002% FAR with 7% FRR.
- **Face** achieves 0.003% FAR with 13% FRR.
- **Voice** can achieve 0.01% FAR with 10% FRR.

From the test results, it is concluded that iris has the lowest FAR compared to other biometric recognition technologies.

In other research (Bowyer, 2009), it was evaluated that the false match rate for iris stands at 1 in 1.2 million using one eye and can be as low as 1 in 1.44 trillion using two eyes. From this, the following evaluation is made:

False Acceptance Rate:

- Iris: Very high
- Fingerprint: High
- Face: Moderate
- Voice: Low

False Rejection Rate:

- Iris: Very high
- Fingerprint: Moderate
- Face: Low
- Voice: Moderate

Resistance to Forgery

There have been forgery attempts for all biometrics In several studies attacks against biometric recognition technologies and forgery methods are analyzed as well as countermeasures to defeat these attacks (Adair, Aimale, & Rowe, 2007; Roberts, 2006; Nixon, 2004; Nixon et al., 2007; "Eyeball Reflexes," 2008; Schuckers, 2009; Cukic, Bartlow, & Bojan, 2005; Reid, 2004; White, 2009).

Compared with other biometric recognition technologies, Iris is considered the most difficult to be forged, as is stated in *Biometrics for Network Security* (White, 2009). The main reason for this advantage of the iris is that biometric data containing the iris are more difficult to be retrieved or captured without the user's knowledge or consent. In order for the capture of the iris biometric data, a high resolution camera should be used, and the user should be properly positioned in order not to let external conditions (such as light) obstruct the data capture. On the other hand, fingerprints can be retrieved if a person touches specific material, where the pattern of the friction ridges can be left on it. Again, specific conditions have to be met; for example, the material has to be specific in order to capture successfully the fingerprint data. However, it is easier to be captured than the iris data. Face and voice are public traits that are easier to be captured compared to iris and fingerprint, for example, with a camera or a voice recorder.

In Jain, Ross, and Pankanti(2006), it is stated that circumvention (the possibility of forgery) is evaluated as:

Resistance to Forgery:

- Iris: Very high
- Fingerprint: Medium
- Face: Low
- Voice: Low

Resistance to Environmental Conditions

Biometric recognition technologies which are assessed (e.g., iris, fingerprint, face, voice) are all in some way affected by environmental conditions:

- **Fingerprint** readers should be clean and they may be affected by dust or moisture.
- **Iris** and **face** may be affected by light.
- **Voice** may be affected by noise.

Therefore, the resistance of each biometric technology would be related to the application for which it is used. If it is used for electronic access conducted at the user's home, then external interferences can be limited. If an application is for access from a public place, then the conditions of the place should be taken into account (e.g., if there is noise or lack of light).

For the purposes of nonrepudiation in electronic transactions, environmental conditions can be controlled. Electronic access can take place at the user's home; therefore, the place can be prepared in order for the biometric technology to be used successfully. Therefore, we consider that all biometric recognition technologies **have equal rating (moderate)** for the provision of nonrepudiation regarding their resistance to environmental conditions. This factor is of medium importance since it does not hinder the provision of nonrepudiation but creates problems to the biometric issuance process.

Resistance to Alteration

Regarding alteration, biometrics may be vulnerable to certain diseases or disabilities:

- **Fingerprint** and **Face** may be damaged from injuries like burning.
- **Iris** can be altered by eye diseases.
- **Voice** cannot be used by mutes.

Therefore, there are situations when all biometrics can be ineffective or unusable. However, the authors consider that such cases are rare and that people with the specific problems are limited. These problems can be overcome if a second biometric is registered and used in cases that the primary biometric is damaged or altered. Therefore, again for this factor the evaluated biometrics are considered to have **equal rating (moderate)**.

USER ACCEPTANCE

In Liu and Silverman (2001), the following evaluation has been conducted regarding user acceptance.

User Acceptance:

- Iris: Medium
- Fingerprint: Medium
- Face: Very high
- Voice: High

At this point, we have evaluated this factor as medium importance for nonrepudiation since it does not violate the principle of nonrepudiation. Also, it can be significantly improved through user awareness, training, and frequent use. When a biometric recognition technology is used for the first time, it may create discomfort to the user and reluctance to use it. However, if the process is explained as well as its relevant benefits, users' attitudes will be different. In a survey where the use of biometrics is evaluated for the provision of nonrepudiation (Lagou & Chondrokoukis, 2009; Lagou, 2010), 69% of the participants (who were all biometric experts) were positive about the use of biometrics for the specific purpose. Many of the participants commented on the users' change of attitude upon explanation of the relevant process and the relevant benefits. Users' acceptability towards biometrics in cases where their use has benefits such as increased security is also evident in the study "Investigation of user acceptance for biometric verification/identification methods in mobile units" (Giarimi & Magnusson, 2002), where the possibility of using biometrics for access in mobile units is explored. In this paper it was concluded that "the results from our investigation clearly show that future users are positive to biometric methods. More exactly, 93% of the students in the study could consider themselves using some kind of biometric method in mobile units. 43% of the students preferred to use a biometric method instead of a PIN-code or password."

Currently, even though biometrics are not widely used, their advantages are recognized, and their feasibility of use is explored in several cases such as passports (European Parliament and Council of the EU, 2009), VISA applications (European Parliament, 2009), blood donors identification (Lux, 2009), and access to electronic health records (Ivon, 2009). Their frequent use will have a positive effect on user acceptance factor.

COST

To evaluate the cost of the biometric recognition technologies under consideration, two research papers have been taken into account: "Automated Biometrics" (Ratha, 2001) and "Biometric Technologies: Security, Legal and Policy Implications" (Rosenzweig, Kochems, & Schwartz, 2004). In paper Ratha, the following evaluation has been conducted regarding sensor cost:

- **Iris**: $3,000
- **Fingerprint:** $100
- **Face:** $50
- **Voice:** $5

In the second research paper (Rosenzweig, Kochems, & Schwartz, 2004), the following estimation has been made (only for biometric readers, without taking into account additional costs):

- **Iris**: $2,000
- **Fingerprint:** $1,000–3,000
- **Face:** $125–500
- **Voice:** Very inexpensive

The significant difference between the two research articles is the cost of the fingerprint. However, the authors of both papers come to the same conclusion regarding compared costs, where biometric technologies are evaluated as:

Cost Effectiveness:

- Iris: Very low
- Fingerprint: Low
- Face: High
- Voice: Very high

TABLE 2 Comparative Evaluation

	Iris	Fingerprint	Face	Voice
FAR	15	12	9	6
FRR	10	9	4	6
Resistance to forgery	15	9	6	6
Resistance to environmental conditions	6	6	6	6
Resistance to alteration	6	6	6	6
User acceptance	6	6	10	8
Cost	1	2	4	5
Total evaluation	**59**	**50**	**45**	**43**

In this evaluation, it must be taken into account that as the usage of a technology increases, costs tend to reduce as it has occurred in other cases such as with PCs and mobile telephones. Therefore, the negative effect of this factor can be overcome. In addition, cost does not affect nonrepudiation, and that is why it is considered to be of low importance for the implementation of the proposed model for the provision of nonrepudiation in electronic transactions.

COMPARATIVE EVALUATION

Taking into consideration the evaluation conducted in the previous section, we estimate the suitability of each biometric recognition technology regarding the provision of nonrepudiation.

Factors' Weights:

- High significance: 3
- Medium significance: 2
- Low significance: 1

Evaluation:

- Very high: 5
- High: 4
- Moderate: 3
- Low: 2
- Very low: 1

Using the scales above and the factors' evaluation conducted, results are shown in Table 2.

Analysis of Table 2 has been conducted in the following way:

Example: *Iris:*

- FAR = Very high * High significance = 5*3 = 15
- FRR = Very high * Medium significance = 5*2 = 10
- Resistance to forgery = Very high * High significance = 5*3 = 15
- Resistance to environmental conditions = Moderate * Medium significance = 3*2 = 6
- Resistance to alteration = Moderate * Medium significance = 3*2 = 6
- User acceptance = Moderate * Medium significance = 3*2 = 6
- Cost = Very low * Low significance = 1*1 = 1

CONCLUSION

Following the analysis conducted, iris provides the most benefits when used for implementing nonrepudiation in electronic transactions. To cover cases where iris cannot be used (e.g., in cases of sickness that has caused damage to the iris), an alternative biometric can be selected. Fingerprint is recommended which, according to the above analysis, is rated as second choice for suitability of a biometric recognition technology for the implementation of the recommended model for the provision of nonrepudiation in electronic transactions.

REFERENCES

Adams, C. and Just, M. (2007). PKI: Ten years later. Available at: http://middleware.internet2.edu/pki04/proceedings/pki_ten_years.pdf

ASIS International. (2008). Information Resources Center. Available at: http://www.asisonline.org/library/glossary/b.pdf

Bowyer, K.W. (2009). Stability of the iris match distribution. *Biometric Consortium Conference*, September 22–24, Tampa, Florida.

Chondrokoukis, G. and Lagou, P. (2009, October). Nonrepudiation: Gap between legislation and practice. The Electronic Journal for Emerging Tools & Applications, pp. 7–10.

Cukic, B. and Bartlow, N. Bojan. (2005). Biometric system threats and countermeasures: A risk-based approach. Biometric Consortium Conference, Crystal City, Virginia. Available at: http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_Ballroom%20B/Cukic_Threats%20and%20countermeasures.pdf

Ellison, C. and Schneier, B. (2000). Ten risks of PKI: What you're not being told about public key infrastructure. Computer Security Journal, 16(1), 1–7.
European Commission (1999). Directive 1999/93/EC.
European Commission. (2008). Amendment of Directive 1999/93/EC
European Parliament and Council of the European Union.. (2009). Regulation (EC) No 444/2009 of the European Parliament and Council, May 28, amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal of the European Union, 6.6.2009.
European Parliament. (2009, March 12). Common consular instructions: Biometric identifiers and visa applications. Official Journal of the European Union
Eyeball reflexes: Security and biometrics that cannot be spoofed. (2008). ScienceDaily, Available at: http://www.sciencedaily.com/releases/2008/09/080904102751.htm
Giarimi, S. and Magnusson, H. (2002). Thesis. Investigation of user acceptance for biometric verification/identification methods in mobile units. Master of Computer and Systems Sciences, Department of Computer Systems Sciences, Stockholm University.
Goulet, W. (2009). Analyzing enterprise PKI deployments. SANS Institute InfoSec Reading Room, August 4. Available from: http://www.sans.org/reading_room/whitepapers/auditing/analyzing_enterprise_pki_deployments_33284
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (1989). ISO 7498-2.
Ivon, N. (2009). Implementation of biometrics and single sign-on for access to electronic health records. *Biometric Consortium Conference 2009*, September 22–24, Tampa, Florida.
Jain, A., Ross, A., and Pankanti, S. (2006, June). Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security, 1(2), pp. 125–143.
Kholmatov, A. and Yanikoglu, B. (2006). Biometric cryptosystem using online signatures. Available at: https://research.sabanciuniv.edu/57/1/3011800000302.pdf
Lagou, P. and Chondrokoukis, G. (2009). Survey on nonrepudiation: Digital signatures vs. biometrics. Information Security Journal, 18(5), 257–266.
Lagou, P. (2010). Nonrepudiation. Draft of PhD Thesis National Science and Technology Council (NIST). Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics (2006). Biometrics overview, August 7. Available from: http://www.biometrics.gov/Documents/BioOverview.pdf
Liu, S. and Silverman, M. (2001, January-February). A practical guide to biometric security technology. Available at: http://www.lfca.net/Reference%20Documents/A%20Practical%20Guide%20To%20Biometric%20Security%20Technology.pdf
Lux, P. (2009). Biometric donor identification at the Indiana Blood Center. *Biometric Consortium Conference 2009*, September 22–24, Tampa, Florida.
Mansfield, T. (2001). Biometric product testing final report. Available at: http://www.cesg.gov.uk/policy_technologies/biometrics/media/bioetricmtestreportpt1.pdf
Nalini, K. Ratha, Senior, A., and Bolle, R.M. (2001). Automated biometrics. *Proceedings of ICAPR-2001*, Rio de Janeiro, Brazil. Available at: http://www.research.ibm.com/ecvg/pubs/ratha-autho.pdf
Nixon, K. Adair (2004). Research & development in biometric anti-spoofing. Available at: http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20PowerPoint%20%204%20NixonBrief.pdf
Nixon, K. Adair, Aimale, V., and Rowe, R.K. (2007). Handbook of biometrics. Springer Science: New York, NY.
Nixon, K. Adair, Aimale, V., and Rowe, R.K. (2007). *Spoof detection schemes*. In: Handbook of biometrics. Available at: www.lumidigm.com/download/Spoof-Detection-Schemes.pdf
Perez, A. (2000). Ten risks of PKI, response. Available at: http://homepage.mac.com/aramperez/responsetenrisks.html
Reid, P. (2004). Biometrics for network security. Pearson Education: Upper Saddle River, NJ.
Roberts, C. (2006). Biometric attach vectors and defenses. Computers & Security, 26(1), 14–25.
Rosenzweig, P., Kochems, A., and Schwartz, A. (2004, June 21). Biometric technologies: Security, legal and policy implications, No. 12. The Heritage Foundation. Available at: http://www.heritage.org/research/reports/2004/06/biometric-technologies-security-legal-and-policy-implications
Schneier, B. (1999). The uses and abuses of biometrics. Communications of the ACM, 42(8).
Schuckers, S. (2009). Liveness detection—LivDet 2009. *Biometric Consortium Conference*, September 22–24, Tampa, Florida.
Shan, L. (2009). The PKI authentication system with the integration of biometric identification and nonsymmetric key technology. *International Symposium on Web Information Systems and Applications (WISA'09)*, May 22–24, Nanchang, China.
White, C. (2009). Biometrics and cyber security key considerations in protecting critical infrastructure – now and in the future. *Biometric Consortium Conference 2009*, September 22–24, Tampa, Florida.
WP3, FIDIS (Future of Identity in the Information Society). (2005). D3.2: A study on PKI and biometrics. Available at: http://www.fidis.net/resources/deliverables/hightechid/int-d32000/

BIOGRAPHIES

Panagiota Lagou is a PhD student in University of Piraeus, Department of Industrial Management. She has a degree in Economics from Athens University of Economics and Business, Department of Economics and a Master Degree in 'Secure Electronic Commerce' from Royal Holloway, University of London. She is currently working in Vodafone Greece S.A. as Senior Information Security and Fraud Analyst.

Gregory P. Chondrokoukis is an assistant professor in the MIS area at the Industrial Management and Technology Department, University of Piraeus. He received his Ph.D., University of Piraeus, Department. of Industrial Management, BSc Business Administration, The Piraeus Graduate School of Industrial Studies. His research interests include E-Commerce, Information Systems, Decision Support and Expert Systems. He participated in more than thirty European Projects in the area of Small Medium Sized Enterprises, Strategic Planning for Business, Human Computer Interaction, Interfaces Design, Industrial Management, E-Commerce, et cetera. He has published over forty publications in the field of Operational Research, Decision Support & Expert Systems and Business Analysis. He was chairman in Public Sector Enterprises.