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

Survey on Nonrepudiation: Digital Signature Versus Biometrics

Panagiota Lagou [a] & Gregory Chondrokoukis [a]
[a] Economics University of Peiraeus , Athens, Greece
Published online: 24 Nov 2009.

To cite this article: Panagiota Lagou & Gregory Chondrokoukis (2009) Survey on Nonrepudiation: Digital Signature Versus Biometrics, Information Security Journal: A Global Perspective, 18:5, 257-266, DOI: 10.1080/19393550903300464

To link to this article: http://dx.doi.org/10.1080/19393550903300464

Information Security Journal: A Global Perspective, 18:257–266, 2009

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393550903300464

Taylor & Francis
Taylor & Francis Group

Survey on Nonrepudiation: Digital Signature Versus Biometrics

Panagiota Lagou and Gregory Chondrokoukis
Economics University of Peiraeus, Athens, Greece

ABSTRACT The scope of this article is to evaluate the provision of nonrepudiation in electronic transactions. For the evaluation of the provision of nonrepudiation, two technological methods are compared: digital signatures and biometrics.

KEYWORDS biometrics, digital signatures, Nonrepudiation

DEFINITIONS

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

- **Information Security:** The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional (ASIS International, 2008).
- **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 International, 2008).
- **Digital signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, for example, by the recipient (Commission of the European Communities, 2006).
- **Nonrepudiation:** It is the principle that provides protection against false denial of having been involved in a communication (ISO and IEC, 1989).

In ISO/IEC 13888-1, definition of nonrepudiation is analyzed in:

1. Nonrepudiation of creation.
2. Nonrepudiation of delivery.
3. Nonrepudiation of knowledge.
4. Nonrepudiation of origin.
5. Nonrepudiation of receipt.
6. Nonrepudiation of sending.
7. Nonrepudiation of submission.
8. Nonrepudiation of transport.

Address correspondence to Panagiota Lagou, Economics University of Peiraeus, Macriyiannis 2, , Agia Paraskevi, PC 15341.
E-mail: paney_lag@yahoo.com

In this article, the term nonrepudiation refers to nonrepudiation of sending, which is the service that is intended to protect against the sender's false denial of having sent a message (ISO and IEC, n.d.).

SCOPE

The scope of this article is to evaluate the provision of nonrepudiation in electronic transactions. Nonrepudiation is required in many existing applications such as e-commerce, e-banking, and e-governance, and its successful provision could lead to the development and enhancement of many more, such as digital contract signing (through the Internet), access to confidential documents and applications (for which now physical presence is required), registration in several activities (for which now physical presence is required), and so forth.

For the evaluation of the provision of nonrepudiation, two technological methods are compared: digital signatures and biometrics. Digital signatures are provided through Public Key Infrastructure (PKI) (Lagou, 2003), and it is the technology currently legally supported for the provision of nonrepudiation (Commission of the European Communities, 2006). The primary disadvantage of PKI relating to the provision of nonrepudiation is the protection of the private key. This disadvantage and others have been identified in many papers (Ellison & Schneier, 2000; Lines, n.d.; McCullagh, 2000) and have been expressed by participants of the survey (responses are included in the analysis of issue.

The authors' recommendation, whose feasibility is explored, is the provision of nonrepudiation by the use of biometric technology and more specifically the iris. The specific infrastructure is recommended to be supported by public sector in each country (the model is briefly described in the next section).

The addressing of weaknesses of digital signatures through the use of biometrics has been identified in other papers as well (WP3, 2005). In the papers "Biometrics and PKI-based digital signatures" (IBG, 2005) and "Biometric cryptosystem using online signatures" (DAON, 2003), it is recommended that the two technological methods are used together. In (IBG, 2005), it is specifically mentioned that "biometric authentication increases the level of nonrepudiation . . ." and in (DAON, 2003) that "biometrics also provide nonrepudiation (an authenticated user cannot deny having done so to some degree because of the difficulty in copying or stealing someone's biometrics)." In this article, biometrics is recommended to be used as a primary method of identity verification with the support of cryptographic methods for the secure distribution of the biometric image.

To accomplish the evaluation of the provision of nonrepudiation through digital signatures and through biometrics, three main areas have been covered:

1. **Digital signatures:** How extensively are digital signatures used? Do users trust digital signatures for the provision of nonrepudiation? This category is required to explore whether the current technological model, which legally supports nonrepudiation, has succeeded in the provision of this principle.
2. **Biometrics:** Is it possible for users to trust biometrics for the provision of nonrepudiation? Which biometric do users prefer for identity verification in electronic transactions? This category is needed to identify users' response towards biometrics for the provision of nonrepudiation.
3. **Iris:** What is the users' opinion regarding the iris as biometric technology? What are considered to be its basic advantages and disadvantages? Questions relating to this area are important in order to explore users' response towards the use of the iris.

MODEL DESCRIPTION

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

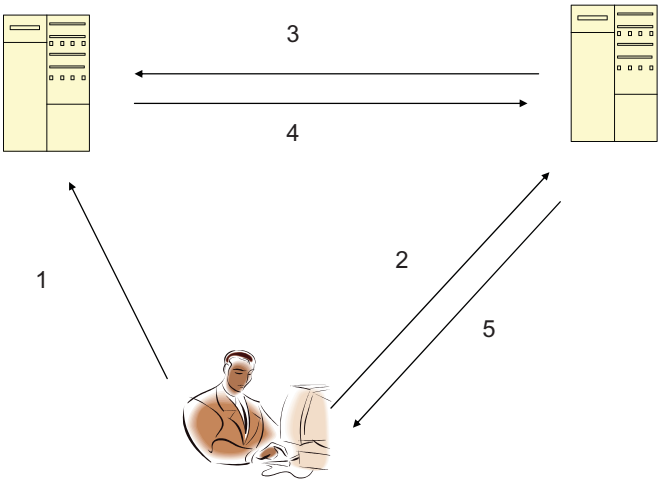

FIGURE 1 Nonrepudiation model through the use of biometrics.

1. The user contacts the public organization that 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 and reserved.
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 (at this step the image of the biometric characteristic can be hashed and then encrypted for improved security).
3. The second transacting party sends the image of the user's biometric characteristic to the public organization for authenticity verification.
4. The organization receives the biometric sample, decrypts it, and compares it to the one 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, 2008).

Advantages of the recommended model for the provision of nonrepudiation include:

- The data created from a biometric are directly derived from the human entity and therefore are with no doubt 'uniquely linked' to the user taking part in a transaction.
- The use of biometrics is more user friendly comparing to the use of 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 (Utah Digital Signature Act, n.d.) This means that periodically the user should enroll again for a new certificate. The enrollment for a biometric only takes place 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.

At this point, it is important to note that digital signatures are not rejected as a technological method for authentication or for many other applications in which they are useful and their operation has proven to be successful. Their ability regarding the addressing of nonrepudiation is their only operation evaluated in this article.

By the description of the recommended model, it can be concluded that information security of the infrastructure can be established by the implementation of appropriate controls and measures. Specifically:

- **Confidentiality:** The digital image of the biometric is encrypted during distribution in order to prevent unauthorized disclosure.
- **Integrity:** The use of a hash function can be used to avoid unauthorized alteration during distribution.
- **Availability:** The possibility of unavailability of the iris, which is the recommended biometric to be used is low. It can only occur in cases of an illness. However, these cases can be addressed by setting a backup biometric, for example, the fingerprint.

A risk assessment of the model is out of the scope of this article and is described in detail in PhD thesis "Nonrepudiation" (Lagou, 2008).

VULNERABILITIES OF DIGITAL SIGNATURES—BIOMETRICS

As with any security model, vulnerabilities exist for both technological methods. The most important ones are identified as follows:

Digital Signatures (Ellison & Schneier, 2000)

- **Unauthorized use of the private key:** As stated in other sections, the private key is stored in a computer or in a device. The user is responsible for providing secure storage for the private key. If the user does not provide adequate protection of the private key, PKI security is violated. This vulnerability has not been addressed and is apparent in other papers (Perez, 2000; Laurie, 2000; Adams & Just, 2007).
- **Inadequate identification of the private key owner:** How is a digital signature linked? Is it with a name? What is the specific attribute that verifies the identity of the user? In the certificate, a name is recorded. However, how about people with the same name? The digital signature cannot be linked directly to the individual, only to the media where it is stored. In Adams & Just

(2007), is the authors state that ". . . applications that rely upon PKI for authentication need to recognize that this issue is not solved by PKI . . ."

- **False registration:** Very good authentication procedure is required to verify the identity of the owner of the private key. This can be implemented. However, since the security of the private key cannot be certified then the owner/user of the digital signature cannot be verified adequately at each usage to provide non repudiation.

Biometrics (Roberts, 2006)

- **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 addressed 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, including (Nixon, 2004; Nixon et al., 2007; Inderscience Publishers, 2008).
- **False enrollment:** Good authentication and enrollment procedures are required. With the implementation of a secure infrastructure, this issue can be addressed.
- **Reuse of provided biometric sample reserved in the reader:** This threat can be addressed by the use of a reader, which does not reserve the biometric data presented upon processing. This threat is not applicable to digital signatures.
- **Biometric destruction:** If the biometric data used are destructed (e.g., by an illness), this can create a problem with the authentication procedure (Schneier, 1999). This problem can be addressed by the provision of an alternative biometric sample, which will be used in such cases. This is addressed by digital signatures as well by the revocation procedure.

From the threats/vulnerabilities presented in this section, unauthorized use of the private key can be compared to biometric spoofing, and false registration and identification of the private key owner can be compared to false enrollment. Again, it is apparent that specifically for the provision of nonrepudiation, biometrics can address the problem of private key protection because biometric data derive directly from the user. Biometric spoofing is a significant problem to be solved, but research is being conducted (Cukic & Bartlow, 2005) to show that countermeasures can be implemented to provide adequate security against this attack.

SURVEY DESIGN

There were 78 questionnaires submitted and used in this research. This survey required feedback from four areas of expertise: Information security, 30; public sector, 19; biometrics, 15; and legal, 14.

Participants were from different organizations/companies. Very few participants worked at the same company (7). For response to the questionnaires, interviews were conducted. In cases where the responder was not a resident of Greece, communication was conducted via email. Pilot interviews were conducted to verify that questionnaire was clear to the participants. Outcomes from pilot interviews were not included in the final results of the survey.

More information security experts were requested to provide feedback since information security is the primary issue under evaluation. However, since the principle of nonrepudiation has to be legally supported, lawyers' evaluations were also needed. In addition, the model recommended is based on the use of biometrics (and that is why biometric experts were included in the survey) and on the ability of the public sector to support this solution (therefore, public sector employees with IT backgrounds were consulted).

ANALYSIS

The questions cover three basic areas in scope:

Digital Signatures

1. Do you think that digital signatures successfully support the principle of non repudiation?
2. Have you or would you ever use digital signatures in an electronic transaction where there is a need for strong authentication (nonrepudiation)?
3. Do you think that there are security issues in PKI (which supports the operation of digital signatures), which prohibit the addressing of nonrepudiation principle?

Biometrics

4. Do you think that biometrics can be used for the provision of nonrepudiation?
5. Have you ever used biometrics for authentication in electronic or physical access?

6. Which biometric technology would you use for the provision of nonrepudiation?

Iris

7. Which you consider to be the primary advantage of iris for the provision of nonrepudiation?
8. Which you consider to be the primary disadvantage of iris for the provision of nonrepudiation?

Digital Signatures

Issue 1 (Figure 2)

Statistics. Regarding the question whether digital signatures successfully support the nonrepudiation principle, 41% gave a positive answer, 19% gave a negative answer, 23% replied "maybe," and 17% responded "I do not know."

Comments/Opinions. An information security expert who answered "Maybe" made the following comment: "Digital signatures are not the only prerequisite for nonrepudiation. There are many other issues (human factor, etc.) which are equally important for the provision of nonrepudiation." Another comment made by an expert in information security who also responded "Maybe" was: "It depends on the strength of the algorithm used." Due to rapid technological evolution, there is always the risk that existing standards that apply to digital signatures' creation may not provide an adequate level of security. An additional comment was: "Public Key Infrastructure is an excellent tool which may be used in combination with other proofs of identity for the provision of non repudiation." This person as well expressed doubts regarding digital signatures' ability to address nonrepudiation principle without the use of another mechanism. In accordance with the previous comments, two biometrics' experts supported their negative opinion, expressing doubts about the security of the private key used for the digital signature creation, through the operation of PKI. This weakness of PKI has been identified (Ellison & Schneier, 2000) from the beginning of its use. However, even though this issue has been identified, still no control has been found to overcome it, and it is the main concern regarding the provision of nonrepudiation as is concluded from the present survey.

Similar doubts to the ones expressed by the participants of the survey have been identified in another survey conducted by the Commission of the European Communities (2006).

Comparison Questions 1–3. At this point, it is interesting to compare the responses of the participants to this question in combination to their responses to question 3, whether there are security issues in PKI that prohibit the addressing of nonrepudiation principle. From the participants who answered "Yes" to Issue 1, 31% think that there are security problems in PKI, 22% replied "I do not know," 22% replied "Maybe," and only 25% said "No."

Issue 2 (Figure 2)

Statistics. This question explores whether people who participated in the survey have or would use digital signatures where strong authentication is required.

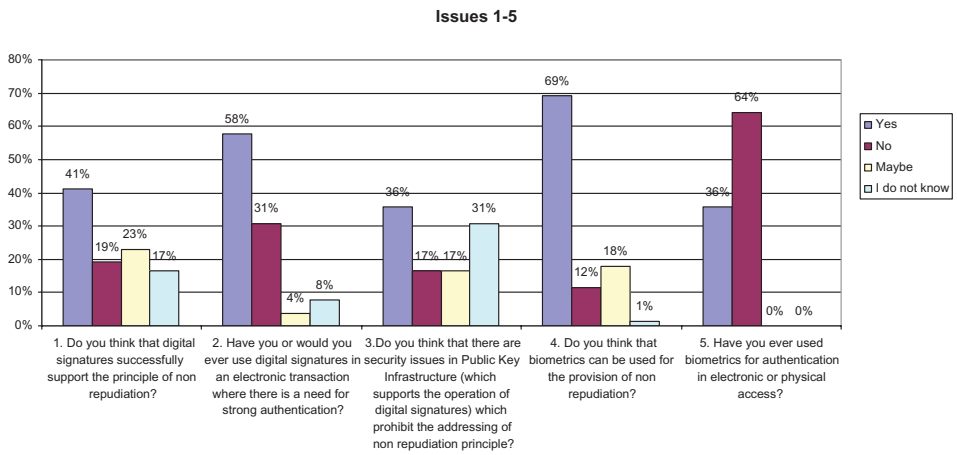

FIGURE 2 Chart of issues 1–5.

Fifty-eight percent stated they have or would use digital signatures for the requested purpose. This means that the majority of the people who participated in the research has experience with the use of digital signatures and yet doubt their use for the provision of nonrepudiation.

Comments/Opinions. It has to be noted, that an information security expert who answered "Yes" in this question added: "I have not done it but I would if I had a digital signature which I would be certain that nobody can access it from my PC." This means that he as well identifies the user's responsibility and important role in the successful operation of PKI regarding the protection of the private key used and would use it only if he could satisfy this requirement. This responsibility is one major weakness of digital signatures. An additional comment, in accordance with the one mentioned above, from a biometric expert who answered "Yes" was: "Yes, but only in combination with another method of authentication like biometrics." Relevant comments were made from other responders.

Issue 3 (Figure 2)

Statistics. Regarding the security of PKI, 36% of the survey participants responded that they think there are security problems in PKI, 17% replied negatively, 17% answered "Maybe," and 31% replied "I do not know."

Comments/Opinions. An information security expert who does not think that there are security problems in PKI mentions: "The problems are not so much technical but they relate to the operation of PKI and the human factor." A biometrics expert made a similar comment. Another information security expert who replied "Maybe" added: "It depends on how the key distribution is conducted, the complexity of security algorithms, the provision of relative roles (who creates, who signs, who distributes digital signatures)." In accordance with these opinions is the comment of a lawyer who states: "Problems tend to occur from the negligent use of the systems by their users (e.g., inadequate protection of their private keys, use or/and storage of the keys in public computers) or from lack of secure access to the users' keys (e.g., remote access through insecure network). An additional danger, which exists for all technological methods, is the probability that an unauthorized third party could manage to break the used algorithm and gain unauthorized access to confidential information. To all cases mentioned, the owner of the private key will be able (under certain circumstances) to repudiate his/her participation in relative actions." However, if a user can claim weakness in protecting his/her private key this creates a problem in the provision of non repudiation.

Taking into account the analysis made in this section, for digital signatures we may come to the conclusion that they are widely used but concerns exist mainly about the physical security of the private key, which is an obstacle in the provision of nonrepudiation.

Biometrics

Issues 4/5 (Figure 2)

Statistics. For biometrics the opposite trend was identified. Only 36% of the people who responded have used this technology but (Issue 5) 69% think that they can be used for the provision of nonrepudiation. Twelve percent gave a negative answer to this question, 18% replied "Maybe," and 1% said "I do not know."

Comments/Opinions. An information security expert who replied "Maybe" in this question made the following comment: "In combination with some other form of authentication, there are ways that biometric data can be altered/ forged. The current technology is never 100% reliable. The writers' opinion is that there are threats against biometrics, but they can be addressed with the implementation of adequate security controls (Lagou, 2008). Another comment made from a professional who answered "Maybe" was: "Due to increased trust that people have on biometric technology, I would be very cautious regarding the risk of disclosure/unauthorized use of my biometric data." A lawyer who gave a positive answer was: "There should be legal framework regarding data protection issues."

It is therefore noted that doubts and concerns are mostly focused on data protection issues, which can be addressed by the implementation of acceptable level of security (Lagou, 2008). It is also apparent that even though biometrics technology is not widely used due to various reasons (e.g., cost, lack of applications), most users trust their operation.

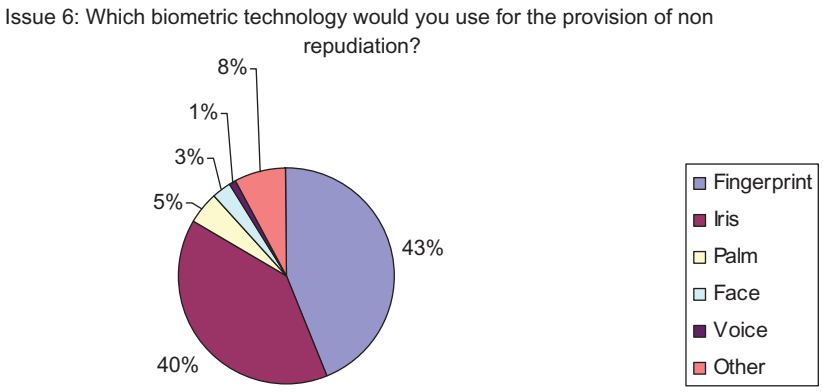

FIGURE 3 Pie of issue 6.

Issue 6 (Figure 3)

Statistics. Responding to the question "Which biometric technology would you use for the provision of non repudiation," 43% replied that they would choose the fingerprint, 40% the iris, and the rest (17%) preferred some other biometric technology. A reason for the preference of fingerprint is considered to be the familiarity that users have with this technology (in comparison to other biometric technologies). From all biometric technologies, fingerprint is used for the longer time period. This means that even though few people use it in everyday activities, its use is known. For example, it is common knowledge that in the physical world, fingerprint is used for identity verification when this is required, for example, to register for a national ID, passport, or in other legal issues (e.g., criminals' arrests). This has as a consequence, when a person is requested to choose a biometric, among others, which he has not used before, to have a preference for the one that he has heard more information about or knows of more applications.

Comments/Opinions. A biometrics expert who chose the fingerprint replied: "The fingerprint has low cost. Voice and face are quite good, but they have high False Acceptance Rate. The other ones are very expensive or have big size." From the provided answer it is obvious that the choice of the fingerprint was based on commercial criteria and not on information security ones. Another interesting opinion that was expressed by another expert who preferred the face as a biometric method was the following: "I would use the face for the provision of nonrepudiation. And this is not because it operates exceptionally well, but because of ease of use (people would see their image combined with the transaction) and because cameras are cheap and can be used by anyone. Regarding iris I would comment that some groups of people would reject the idea just because iris is so unique. They may not want their data to be used for any other purpose that they do not approve of." As it is obvious from this reply, the reasons that this expert chose another biometric technology than the iris are again mainly commercial. It has to be noted that in the question regarding the main advantage of the iris (Issue 7), this person replied that it is the small possibility of forgery. A very interesting comment made by a lawyer was: "Any of the mentioned biometric technologies in combination with adequate controls would be possible to cover the legal term of the advanced digital signature (which is legally capable of providing non repudiation)." She also stated that the law provides several prerequisites which can be satisfied by biometric technology and not necessarily by digital signatures.

Comparison Questions 6–7. At this point, it has to be noted from experts who took part in the survey and chose other biometric than the iris, 68% replied that they consider small possibility of forgery the main advantage of iris. This quality of the iris is considered to be the primary condition for the implementation of a model for the provision of non repudiation.

Most experts who participated in the survey have not used biometrics. Nevertheless, they are positive toward their use for the provision of nonrepudiation. The biometric technology which most of them prefer is the fingerprint, and second choice is the iris.

Iris

Issue 7 (Figure 4)

Statistics. Despite that most users are more familiar with fingerprint, 74% responded that they consider small possibility of forgery the main advantage of the iris. As has been noted, this characteristic is a primary requirement for the choice of a biometric technology for the provision of nonrepudiation, which is satisfied by the iris according to the provided replies. It has to be noted that tests have been conducted that have identified iris as the biometric which has 0 FAR (Mansfield, 2001) (or very low in comparison to other biometrics), a result that is in accordance with experts' responses to the current survey.

Issue 8 (Figure 5)

Statistics. Regarding the question "Which you consider to be the primary disadvantage of the iris regarding the provision of nonrepudiation?" 40% stated its high cost, 19% lack of user acceptability, 22% data protection issues, 17% corruption possibilities (e.g., from an illness), and 3% some other reason. From the replies to this question, probably the reasons can be concluded why some participants did not chose iris for the provision of nonrepudiation. It is a positive sign that the majority think that the main disadvantage of iris is high cost, since this is a commercial issue that can be addressed and not an information security problem. Doubts were also expressed regarding data protection issues, which mostly concern the worries and inconvenience of users to "give" and store the data which consist of their biometric characteristics. These doubts are not only related to the iris but also have been expressed for all biometrics.

At this point, it has to be noted that concerning the use of the iris, additional disadvantages could exist such as the Failure to Enroll rate (FER), which can be higher in comparison to other biometrics.

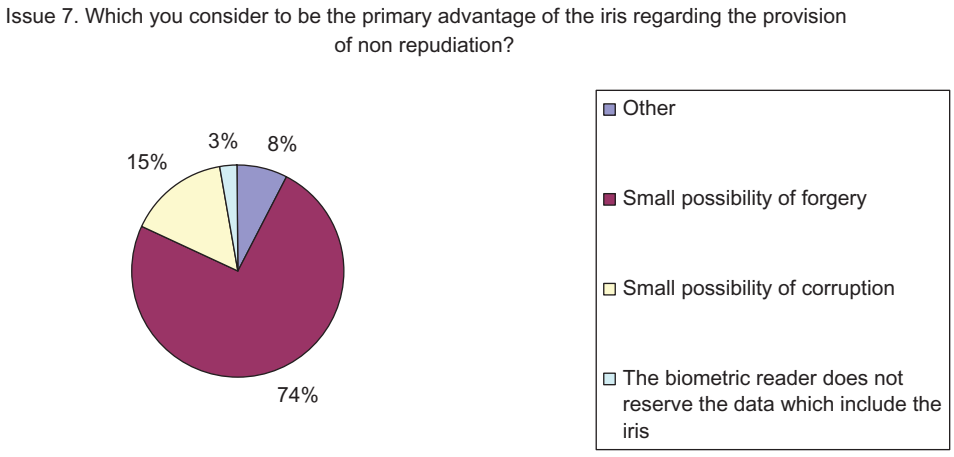

FIGURE 4 **Pie of issue 7.**

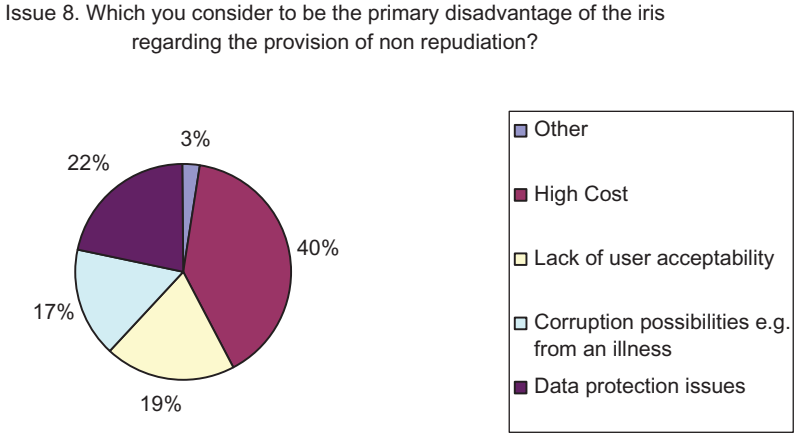

FIGURE 5 **Pie of issue 8.**

Taking into account three different tests conducted, the FER for iris has been calculated to be 0.5% (Mansfield, 2001), 1.4% (IBG, 2006), and 1.61% (Kholmatov & Yanikoglu, 2006), depending on the technological method or device used for iris recognition. For the provision of nonrepudiation, it is emphasized that the primary condition that needs to be met is a small possibility of forgery. As a secondary but still important condition, the level of FER accomplished by the iris recognition system is acceptable for the specific model. In addition, it is considered that the current FER can be improved by more user friendly devices, users' awareness, and increased use of the specific technology.

It is obvious that the experts who participated in the survey trust iris regarding the provided level of security, and their doubts concern other issues such as cost and user acceptability which can be overcome with the implementation of appropriate controls.

Specifically, it is considered that cost of a technology relates to its use. The more a technology is used, the lower its price. Examples of this are PCs and mobile telephones. For both of these technologies, their prices have been reduced over time. User acceptability toward biometrics can also be improved through frequent use and proper awareness. If biometrics is used to facilitate access and improve security in applications, users will be more favorable toward this technology. This is 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."

CONCLUSIONS

From the survey conducted, the following conclusions can be made:

1. **Digital signatures:** Digital signatures have not succeeded into addressing the requirements which are needed for the provision of non repudiation. Even though they legally support this principle, users have concerns concerning their use for the specific purpose (due to weaknesses such as the physical security of the private key).
2. **Biometrics:** Even though biometrics technology is not widely used, users trust their operation and are positive regarding their use for the provision of nonrepudiation. Fingerprint is the biometric which most users would use to provide strong authentication in electronic transactions.
3. **Iris:** Iris technology is considered to be the most difficult to be forged, which is the most important prerequisite for the principle of nonrepudiation. Issues that were raised and need to be overcome are high cost and users' hesitation to provide their biometric characteristics (this issue exists for all biometric technologies).

ABOUT THE AUTHORS

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. Chondrocoukis 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.

BIBLIOGRAPHY

Adams, C., and Just, M. (2007). PKI: Ten years later. University of Ottawa, http://whitepapers.zdnet.com/abstract.aspx?docid=352373

ASIS International (2008). Information Resources Center.

Commission of the European Communities. (2006). Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures.
DAON (2003). Biometrics and PKI based digital signatures.
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.
Giarimi, S., and Magnusson, H. (2002). 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.
Inderscience Publishers. (2008). Eyeball reflexes: Security and biometrics that cannot be spoofed. *ScienceDaily*.
International Biometric Group (2005). Independent testing of iris recognition technology.
International Biometric Group. (2006). Comparative biometric testing.
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (1989). ISO 7498-2.
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), (2009) ISO 13888-1.
Kholmatov, A., and Yanikoglu, B. (2006). Biometric cryptosystem using online signatures. Sabanci University, Faculty of Engineering and Natural Sciences, Istanbul, Turkey.
Lagou, P. (2008). Nonrepudiation. Draft, PhD Thesis. Economics University of Peiraeus, Athens, Greece.
Lagou, P. (2003). Conference 'eAWARe: e-Awareness for Europe: Digital awareness and the security of the citizen in Europe, *Securing Electronic Commerce with Digital Certificates*.
Laurie, B. (2000). Seven and a half nonrisks of PKI: What you shouldn't be told about public key infrastructure. http://www.apache-ssl.org/7.5things.txt
Mansfield, T. (2001). Biometric product testing final report.
McCullagh, A. (2000). Nonrepudiation in the digital environment. *First Monday*, 5(8).
Nixon, K. (2004). Research & development in biometric anti-spoofing. www.biometric.org.
Nixon, K., Adair, A.V., and Rowe, R.K. (2007). *Handbook of Biometrics* (chapter 20), pp. 403–423. http://homepage.mac.com/aramprez/responsetenrisks.html
Perez, A. (2000). Ten risks of PKI, response. Boston, MD: Springer.
Roberts, C. (2006). Biometric attack vectors and defenses.Computers & Security, 26(1), 14–25.
Schneier, B. (1999). The uses and abuses of biometrics. *Comm. ACM*, 42(8), 136.
Utah Digital Signature Act. Utah Codes 46-3-104 & 46-3-307.
WP3, FIDIS (Future of Identity in the Information Society). (2005). D3.2: A study on PKI and biometrics. http://www.fidis.net/resources/deleverables/hightechid/int-d32000/