EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

Non-Repudiation By The Use of Biometrics—Risk Analysis

Panagiota Lagou & Gregory P. Chondrokoukis

Published online: 05 Jun 2012.

To cite this article: Panagiota Lagou & Gregory P. Chondrokoukis (2012) Non-Repudiation By The Use of Biometrics—Risk Analysis, EDPACS: The EDP Audit, Control, and Security Newsletter, 45:6, 5-21, DOI: 10.1080/07366981.2012.683986

To link to this article: http://dx.doi.org/10.1080/07366981.2012.683986

NON-REPUDIATION BY THE USE OF BIOMETRICS—RISK ANALYSIS

PANAGIOTA LAGOU and
GREGORY P. CHONDROKOUKIS

Abstract. A model is recommended for the provision of non-repudiation by the use of biometrics. A risk analysis of the recommended model is conducted in order to evaluate its feasibility and secure operation.

DEFINITIONS

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

1. **Non-repudiation:** It is the principle that provides protection against false denial of having been involved in a communication (ISO 7498-2, 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 International 2010, p. 6).
3. **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 (ISO 7498-2, 1989).

SCOPE

According to legislation (Directive 1999/93/EC, 1999; European Commission, 2008; European Parliament and Council of the European Union, 2009) non-repudiation is addressed by digital signatures. However, significant issues in the operation of digital signatures prohibit the efficient provision of non-repudiation as it has been identified in several papers (Ellison & Schneier, 2000; Perez, 2000; Adams & Just, 2007; Chondrokoukis & Lagou, 2009). A business model is recommended for this purpose by the use of biometrics. A risk analysis is conducted in order to identify potential risks, controls to address the risks, and evaluate the feasibility of using biometrics for non-repudiation.

It has to be noted that the scope of this analysis is to verify security of a model for non-repudiation. Other factors like users' acceptance, cost, and data protection issues have not been analyzed.

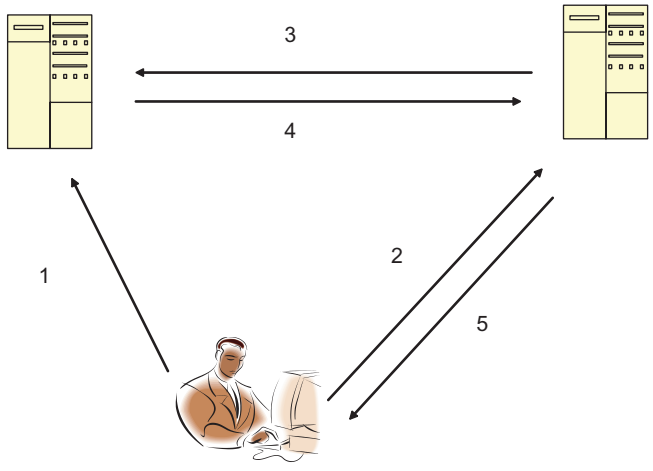
NEED FOR NON-REPUDIATION

Due to wide applications development in the Internet for communication and transactions, there is a strong need for non-

repudiation of users. Some relative cases, in which need for non-repudiation has been identified, are the following:

1. **Internet banking:** Banking sector is a major area that uses the Internet to facilitate customer transactions. Specifically because these transactions are financial, the impact of making transactions with the wrong user is high. At this moment, Internet banking is conducted without implementation of non-repudiation and this vulnerability limits its use (Reserve Bank of India, 2001).
2. **Business to business e-commerce:** Non-repudiation is also required for business-to-business transactions. Lack of non-repudiation has as a consequence slow development or complete obstruction of the applications' use. Such applications can be the evaluation and selection of vendors through Internet, vendors' payment as well as online auctions (Mahadevan & Venkatesh, 2000).
3. **Mobile payments:** Wide use of mobile telephones facilitates the use of mobile transactions. Such transactions can be of small amounts such as toll fees or parking or big transactions like buying and selling of stocks. Since non-repudiation is not implemented, users are reluctant to conduct such transactions and when they are used, transacting parties can be vulnerable to fraud (Ou & Ou, 2008).
4. **Electronic invoices:** Electronic invoices system is used widely. Nevertheless, non-repudiation is not implemented. In this case there is an increased risk of fraud. In Taiwan, electronic invoices system is used since 2004 in order to decrease cost of paper used. Public Key Infrastructure is used without the provision of non-repudiation (Ou & Ou, 2008).
5. **Products deliveries:** In case the dispatch notes have to be sent through the Internet, the verification of the sender's identity is significant. At this moment in relative applications, Public Key Infrastructure is used but weaknesses have been identified (Onieva, Zhou, Lopez, & Carbonell, 2004).

Figure 1 ***Non-repudiation model through the use of biometrics.***



MODEL DESCRIPTION

The recommended model is described briefly.

Steps which are shown in Figure 1 are:

1. The user contacts the public organization, which supports the infrastructure for the provision of non-repudiation through the use of biometrics and goes through the registration procedure, under which a biometric sample is recorded. The registration process should be conducted in 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 an impersonation. The biometric sample linked with the user identity is stored in a database. Strict security controls should be implemented in order 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 that is stored. If it matches, a positive reply is sent. If it does not match then a negative reply is sent.

The second transacting party has now verified the identity of the first transacting party and proceeds with the transaction (Lagou, 2010; Lagou & Chondrokoukis, 2009).

RISK ANALYSIS

In order to address the problem of lack of non-repudiation and verify that the recommended model is feasible a risk analysis has been conducted.

Main Characteristics of the Risk Analysis

The risk analysis that has been conducted has the following characteristics:

- **It is high level.** It analyzes administrative and technical aspects of the model in high level and not in low technical level. This analysis focuses on the processes that support the recommended model, the technical security controls as well as the roles of the employees who participate in the model's operation.
- **It is qualitative.** In comparison to quantitative analysis which is based on ratings and historical data, the present analysis is based on risk scenarios, which determine the evaluation and prioritization of the recommended security controls.

- **Use of Risk Scenarios.** The risk analysis could include for each phase, the relative threats, vulnerabilities, and impact. For facilitation, hypothetical risk scenarios will be used that include these three elements and that can be used as reference in order to justify the selection of the security controls.
- **It is based on the asset's lifecycle.** The analysis is conducted evaluating each step of the recommended model, which is each phase of the biometric's lifecycle. Each phase will be described and analyzed regarding the relative risk level.

For this risk analysis, the principles and requirements that are included in ISO/IEC 17799 (2000) and the updated ISO/IEC 27001 (2005) have been taken into account.

Biometric Lifecycle

The biometric lifecycle includes the following phases:

1. **Registration.** The user/citizen comes into contact with the public organization and conducts the registration of his/her biometric sample. *(step 1 of the recommended model)*
2. **Storage.** Digital data that consist of the biometric sample are captured during registration and stored in a database. *(step 1 of the recommended model)*
3. **Transfer.** Digital data that consist of the biometric sample are transferred for the user's identity verification through an electronic communication channel. *(steps 2, 3, 4 of the recommended model)*
4. **Biometric reader.** A biometric reader is used for the biometric sample recording and its comparison to the stored biometric. *(step 2 of the recommended model)*
5. **Destruction.** The biometric sample should be destroyed when no longer needed. *(this phase is not included in any step of the recommended model)*

Risk Evaluation

In order to evaluate feasibility of the recommended model, relative risks should be identified. The following criteria are used:

- Which security principles each risk affects (**confidentiality, integrity, availability**). For the feasibility of the recommended model, confidentiality and integrity are of high significance whereas availability is of medium significance.
- **Occurrence Probability:** How possible is the occurrence of each risk. The evaluation of this parameter will be made in three scales: high, moderate, low. It is noted that occurrence probability is estimated taking into account the operation of the model without the implementation of recommended controls.

Final risk evaluation will be in five scales:

- **High.** A risk is considered high if it affects more than two security principles and occurrence probability is high or medium.
- **High to moderate.** A risk is considered high to moderate if it affects more than two security principles and occurrence probability is low.

Table 1 ***Risks***

Risk Scenarios	Confidentiality	Integrity	Availability	Occurrence probability	Risk level	Applicable phase
Risk Scenario 1: False user identity verification.		√		Moderate	Moderate	Phase 1: Registration
Risk Scenario 2: Storage of false biometric data (owned by another user).		√	√	Moderate	High	Phase 1: Registration
Risk Scenario 3: Incomplete/ unsuccessful storage of the biometric sample.		√	√	High	High	Phase 1: Registration
Risk Scenario 4: Alteration of the biometric sample by an employee of the public organization.		√		High	Moderate	Phase 1: Registration
Risk Scenario 5: False recording of the user's identity by an employee of the public organization.		√	√	Moderate	High	Phase 1: Registration
Risk Scenario 6: Alteration of the biometric sample through unauthorized logical access during registration.		√	√	Low	High to moderate	Phase 1: Registration
Risk Scenario 7: Inability to conduct the registration process due to unavailability of the required software or hardware equipment.			√	Low	Low	Phase 1: Registration
Risk Scenario 8: Provision of forged/altered biometric sample by the user.		√		Low	Low	Phase 1: Registration
Risk Scenario 9: Denial of service attack.			√	Moderate	Moderate to low	Phase 2: Storage
Risk Scenario 10: Malicious code attack towards the network.		√	√	High	High	Phase 2: Storage
Risk Scenario 11: Database unavailability (where the biometric samples are stored).			√	Low	Low	Phase 2: Storage

(*continues*)

Table 1 *(Continued)*

Risk Scenarios	Confidentiality	Integrity	Availability	Occurrence probability	Risk level	Applicable phase
Risk Scenario 12: Alteration of the biometric samples which are stored in the database through unauthorized logical access.	√	√	√	Moderate	High	Phase 2: Storage
Risk Scenario 13: Alteration of the biometric samples which are stored in the database through unauthorized activity by authorized employees.		√	√	Moderate	High	Phase 2: Storage
Risk Scenario 14: Copy and use of a user's biometric sample through unauthorized logical access.	√			Moderate	Moderate	Phase 2: Storage
Risk Scenario 15: Copy and use of a user's biometric sample through unauthorized activity by authorized employees.	√			High	Moderate	Phase 2: Storage
Risk Scenario 16: Alteration of the stored biometric data through unauthorized remote logical access.		√	√	Low	High to Moderate	Phase 2: Storage
Risk Scenario 17: Deletion of audit log files by an unauthorized party.	√		√	Low	High to Moderate	Phase 2: Storage
Risk Scenario 18: Alteration of audit log files by an unauthorized party.	√	√		Low	High to Moderate	Phase 2: Storage
Risk Scenario 19: Alteration of audit log files by authorized employees.	√	√		Moderate	High	Phase 2: Storage
Risk Scenario 20: Incomplete recording of all required information of a transaction/ activity in the audit logs.		√		High	Moderate	Phase 2: Storage

(*continues*)

Table 1 *(Continued)*

Risk Scenarios	Confidentiality	Integrity	Availability	Occurrence probability	Risk level	Applicable phase
Risk Scenario 21: Copy and use of a user's biometric sample through unauthorized logical access to the electronic communication channel.	√			Moderate	Moderate	Phase 3: Transfer
Risk Scenario 22: Alteration of the stored biometric data through unauthorized logical access to the electronic communication channel.		√		Moderate	Moderate to low	Phase 3: Transfer
Risk Scenario 23: Copy and use of a user's biometric sample through unauthorized logical access to the second transacting party server.	√			Moderate	Moderate	Phase 3: Transfer
Risk Scenario 24: Alteration of the stored biometric data through unauthorized logical access to the second transacting party server.		√	√	Moderate	High	Phase 3: Transfer
Risk Scenario 25: Recreation of a user's biometric sample through trails which have remained in the biometric reader.	√			Moderate	Moderate	Phase 4: Biometric Reader
Risk Scenario 26: Disclosure of confidential or sensitive information through documentation which has been thrown to trash. This information may be users confidential information, technical manuals or processes' descriptions, whose knowledge can facilitate the materialization of an attack.	√			Moderate	Moderate	Phase 5: Destruction

(*continues*)

Table 1 *(Continued)*

Risk Scenarios	Confidentiality	Integrity	Availability	Occurrence probability	Risk level	Applicable phase
Risk Scenario 27: Disclosure of confidential or sensitive information through restoration by magnetic media (eg. hard disk) from which information has been deleted.	√			Moderate	Moderate	Phase 5: Destruction
Risk Scenario 28: Storage of inactive users' data in the database. High volume of data may affect the database operation.			√	Low	Low	Phase 5: Destruction

- **Moderate.** Moderate risk is the one that affects confidentiality or integrity and occurrence probability is high or moderate.
- **Moderate to low.** In this category risks will be included that affect availability and occurrence probability is high or moderate.
- **Low.** In this category risks will be included that affect availability and occurrence probability is low.

Taking into account the above evaluation criteria and weights, risk analysis is included in Table 1.

In order for the recommended model to be able to operate securely, risks that have been identified and evaluated should be addressed by security controls. Evaluation of controls is made as follows:

- **Priority 1:** Recommended controls that address high or high to moderate risks.
- **Priority 2:** Recommended controls that address moderate or moderate to low risks.
- **Priority 3:** Recommended controls that address low risks.

Recommended controls are evaluated accordingly (Table 2).

From the risk analysis conducted, **28** risks and **50** controls are identified. **Eleven** risks affect confidentiality, **16** risks affect integrity, and **14** risks affect availability. Each phase's risks and controls are shown in Figures 2 and 3.

CONCLUSIONS

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

Table 2 ***Controls***

Recommended Controls	Relative risk scenarios	Total risk	Evaluation (prioritization)	Applicable phase
Recommended Control 1: Registration should be conducted through the user's physical presence in the premises of the organization.	Risk Scenarios 1, 2	Moderate	2	Phase 1: Registration
Recommended Control 2: The user should show his/her national ID card, passport or driver's license for identity verification.	Risk Scenario 1	Moderate	2	Phase 1: Registration
Recommended Control 3: Employees, responsible for the conduct of the registration process, should be well trained in order to avoid errors or omissions that may create problems to the process.	Risk Scenarios 1, 2	High to Moderate	1	Phase 1: Registration
Recommended Control 4: Manuals should be created where the registration process is described in detail.	Risk Scenarios 2,3, 5	High	1	Phase 1: Registration
Recommended Control 5: Before registration, clear instructions should be provided to the user regarding the registration process (e.g., How he should be positioned in order for the biometric data to be recorded efficiently)	Risk Scenario 3	High	1	Phase 1: Registration
Recommended Control 6: The biometric reader should be able to check whether the biometric data recorded are adequate. In case insufficient biometric data is recorded an alarm should be activated and the registration process should be terminated.	Risk Scenario 3	High	1	Phase 1: Registration
Recommended Control 7: In case the registration is unsuccessful and is terminated, the system should delete the recorded data and the registration should start again.	Risk Scenario 3	High	1	Phase 1: Registration
Recommended Control 8: Testing should be conducted upon conclusion of the registration process in order to verify the successful recording of the biometric data.	Risk Scenario 3	High	1	Phase 1: Registration
Recommended Control 9: Testing should be conducted in an offline environment that cannot be affected by external threats.	Risk Scenarios 3, 6	High	1	Phase 1: Registration

(*continues*)

Table 2 ***(Continued)***

Recommended Controls	Relative risk scenarios	Total risk	Evaluation (prioritization)	Applicable phase
Recommended Control 10: Employees who undertake sensitive roles should go through a screening check before employment in order to verify trustworthiness. This check can include criminal record submission, verification of academic and/or professional credentials, and more.	Risk Scenarios 4, 13, 15, 19	High to Moderate	1	Phase 1: Registration, Phase 2: Storage
Recommended Control 11: Strict segregation of duties should be enforced when sensitive activities are conducted.	Risk Scenarios 4, 13, 15	High to Moderate	1	Phase 1: Registration, Phase 2: Storage
Recommended Control 12: Registration should be conducted in an offline environment. Biometric sample will be then transferred to the database where it will be stored.	Risk Scenario 6	High to Moderate	1	Phase 1: Registration
Recommended Control 13: Back up hardware equipment should be maintained for all systems that support sensitive operations.	Risk Scenarios 7, 11	Low	3	Phase 1: Registration, Phase 2: Storage
Recommended Control 14: Strict and cautious selection of used software and hardware.	Risk Scenarios 7, 11	Low	3	Phase 1: Registration, Phase 2: Storage
Recommended Control 15: Software and hardware used should be compliant with commonly accepted standards.	Risk Scenarios 7, 11	Low	3	Phase 1: Registration, Phase 2: Storage
Recommended Control 16: Frequent maintenance of the software and hardware equipment should be conducted.	Risk Scenarios 7, 11	Low	3	Phase 1: Registration, Phase 2: Storage
Recommended Control 17: The user should be requested to conduct some moves in order to ensure that a false biometric is not presented.	Risk Scenario 8	Low	3	Phase 1: Registration
Recommended Control 18: Firewalls should be used to filter incoming traffic.	Risk Scenarios 9, 10, 11	Moderate	2	Phase 2: Storage
Recommended Control 19: Intrusion detection system should be used.	Risk Scenarios 9, 10, 11	Moderate	2	Phase 2: Storage
Recommended Control 20: In network level load balancing should be conducted.	Risk Scenarios 9, 10, 11	Moderate	2	Phase 2: Storage

(*continues*)

Table 2 *(Continued)*

Recommended Controls	Relative risk scenarios	Total risk	Evaluation (prioritization)	Applicable phase
Recommended Control 21: Antivirus should be used.	Risk Scenario 10	High	1	Phase 2: Storage
Recommended Control 22: Incremental and full back up should take place to ensure availability.	Risk Scenario 11	Low	3	Phase 2: Storage
Recommended Control 23: A disaster recovery site should exist.	Risk Scenario 11	Low	3	Phase 2: Storage
Recommended Control 24: A business continuity plan should exist.	Risk Scenario 11	Low	3	Phase 2: Storage
Recommended Control 25: Access to the database should be controlled and provided only to employees who need it to conduct their work.	Risk Scenarios 12, 13, 14, 15	High to Moderate	1	Phase 2: Storage
Recommended Control 26: Strict password policy should be enforced. Passwords should: • Be at least 8 characters • Be stored hashed • Contain at least 1 character and 1 number • Be case sensitive • Not be at any time displayed in clear test. • Include a password verification procedure (at least twice) • Not be the user name • Not contain more than 2 consequent same characters • Only be changed upon the password verification has been conducted • Only be reset by system administrator • No hard-coded passwords allowed (i.e., service/ application user passwords displayed in source code) • The system should enforce the change of default passwords at first login • The system should not allow the use of the last 5 passwords	Risk Scenarios 12, 14	High to Moderate	1	Phase 2: Storage

(*continues*)

Table 2 *(Continued)*

Recommended Controls	Relative risk scenarios	Total risk	Evaluation (prioritization)	Applicable phase
• The system should enforce periodic password change (max 2 months)				
Recommended **Control 27:** All security patches and fixes published by the vendor should be immediately installed.	Risk Scenario 12	High	1	Phase 2: Storage
Recommended **Control 28:** Cross-database ownership chaining should not be allowed.	Risk Scenario 12	High	1	Phase 2: Storage
Recommended **Control 29:** Database administration should be conducted by a low privileged account.	Risk Scenario 12	High	1	Phase 2: Storage
Recommended **Control 30:** Alerts should be activated for activities that can be suspicious regarding the security of the database.	Risk Scenario 12	High	1	Phase 2: Storage
Recommended **Control 31:** Periodic checks should be activated in the database checking privileges on all system and non system objects.	Risk Scenario 12	High	1	Phase 2: Storage
Recommended **Control 32:** Periodic checks should be activated in the database checking all users' privileges.	Risk Scenario 12	High	1	Phase 2: Storage
Recommended **Control 33:** Audit logs should be reserved where all access and activity conducted in the database is recorded.	Risk Scenarios 13, 15	High to Moderate	1	Phase 2: Storage
Recommended **Control 34:** Audit logs should be periodically reviewed.	Risk Scenarios 13, 15	High to Moderate	1	Phase 2: Storage
Recommended **Control 35:** Audit logs should include in the least the following information: • User name • Workstation ID • Date and time of access or activity • Successful and unsuccessful access attempts • Files or programs which the user accessed or used • Privileged operations (i.e., use of admin/ superuser accounts)	Risk Scenario 13	High	1	Phase 2: Storage

(*continues*)

Table 2 ***(Continued)***

Recommended Controls	Relative risk scenarios	Total risk	Evaluation (prioritization)	Applicable phase
• Updates/changes to userID access rights • Print commands • Deletion or alteration attempts of important files				
Recommended Control 36: Security log files shall be protected against manual modification or deletion even by the superuser.	Risk Scenarios 13, 19	High	1	Phase 2: Storage
Recommended Control 37: A backup biometric should be defined and registered in order to be used if the primary biometric is forged or damaged.	Risk Scenarios 14, 15	Moderate	2	Phase 2: Storage
Recommended Control 38: There should be a documented procedure of steps to be followed in case security of the biometric is violated. The biometric sample should be deleted from the database, his/her owner should be informed, who should be invited to the organization's premises to provide consent for the backup biometric to be used.	Risk Scenarios 14, 15	Moderate	2	Phase 2: Storage
Recommended Control 39: Biometric samples should be stored in the database encrypted.	Risk Scenarios 14, 15	Moderate	2	Phase 2: Storage
Recommended Control 40: Remote access should not be allowed. If it is required for business operation, it should be conducted through an encrypted communication channel (e.g., Virtual Private Network [VPN]) or by using two-actor authentication.	Risk Scenario 16	High to Moderate	1	Phase 2: Storage
Recommended Control 41: Access to audit logs should be restricted to accounts with administrative privileges.	Risk Scenarios 17, 18	High to Moderate	1	Phase 2: Storage
Recommended Control 42: Communication channels should be encrypted (e.g., via Secure Sockets Layer [SSL] 128 bits).	Risk Scenarios 21, 22	Moderate	2	Phase 3: Transfer
Recommended Control 43: The biometric sample should be encrypted using a	Risk Scenarios 23, 24	High to Moderate	1	Phase 3: Transfer

(*continues*)

Table 2 *(Continued)*

Recommended Controls	Relative risk scenarios	Total risk	Evaluation (prioritization)	Applicable phase
symmetric algorithm and the key should only be known to the database, where decryption will be conducted for authenticity verification. Upon verification, the server of the second transacting party will receive a positive response from the database and the transaction will be conducted. Additionally, the server of the second transacting party will reserve log files of the transaction.				
Recommended Control 44: The biometric reader should be tamper-resistant.	Risk Scenario 25	Moderate	2	Phase 4: Biometric Reader
Recommended Control 45: For each biometric reader it is feasible to configure False Rejection Rate (FRR) and False Acceptance Rate (FAR). For the specific analysis, FAR is of high importance and it must be as low as possible, configuration should be such that FAR is the lowest possible even if FRR is high.	Risk Scenario 25	Moderate	2	Phase 4: Biometric Reader
Recommended Control 46: Shredders should be used for document destruction that includes confidential and sensitive information.	Risk Scenario 26	Moderate	2	Phase 5: Destruction
Recommended Control 47: Information security awareness should be conducted frequently for employees.	Risk Scenario 27	Moderate	2	Phase 5: Destruction
Recommended Control 48: Degaussers should be used for the deletion of information from magnetic media.	Risk Scenario 27	Moderate	2	Phase 5: Destruction
Recommended Control 49: A documented procedure should exist for the deletion of a biometric from the database. This procedure should include deactivation request and the user's signed consent.	Risk Scenario 28	Low	3	Phase 5: Destruction
Recommended Control 50: Restoration of deleted biometric samples should not be possible.	Risk Scenario 28	Low	3	Phase 5: Destruction

Figure 2 ***Phases—risks.***

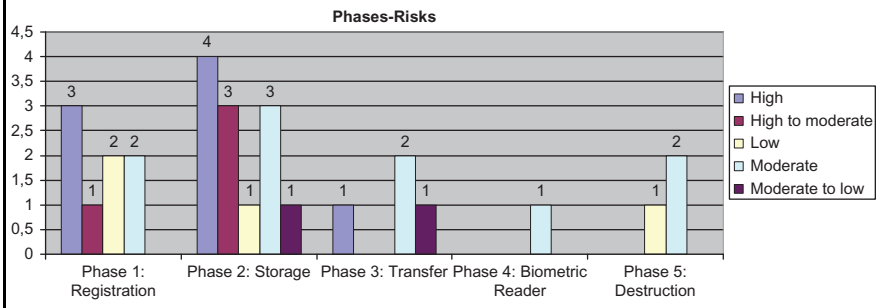
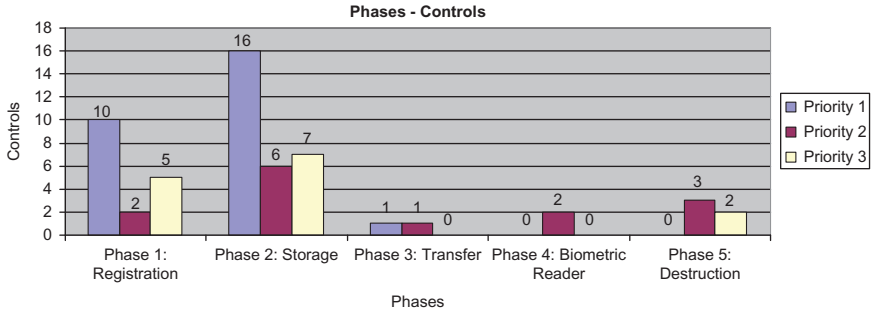


Figure 3 ***Phases—controls.***



1. Most risks are identified in **storage phase** (**4** high, **3** high to moderate, **1** moderate to low, **3** moderate, **1** low). This means that this is the phase in which security should be mostly taken into consideration.
2. Most recommended controls address risks in the **storage phase** (**16** priority 1, **6** priority 2, **7** priority 3).
3. All identified risks were addressed by relevant recommended controls. **There is no risk that cannot be addressed**.
4. The user was not the actioneer or implementer of any of the recommended controls. This means that no additional actions are required by the user for the successful and secure operation of the recommended model.

From the above, it can be derived that the successful and secure implementation of the recommended model is feasible.

References

Adams, C., & Just, M. (2007). PKI: Ten years later. Retrieved from http://middleware.internet2.edu/pki04/proceedings/pki_ten_ years.pdf

ASIS International, Information Resources Center. (2010, June). International glossary of security terms. Retrieved from www.asisonline.org/library/glossary/s.pdf

Chondrokoukis, G., & Lagou, P. (2009, October). Nonrepudiation: Gap between legislation and practice. *The Electronic Journal for Emerging Tools & Applications*, 7–10. Reserve Bank of India, Report on Internet Banking, 2001. Retrieved from http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/21595.pdf

Commission (IEC). (2000). ISO/IEC FDIS 17799, Information technology—Code of practice for information security management.

Commission (IEC). (2005). ISO/IEC FDIS 27001, Information technology, Security techniques, Information security management systems, requirements.

European legislation European Commission. (1999). Directive 1999/93/EC.

European Commission (2008) Amendment of Directive 1999/93/EC. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:EN:PDF

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.

Ellison, C., & Schneier, B. (2000). Ten risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal*, *16*(1), 1–7.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (1989). ISO 7498-2.

Lagou, P. (2010). *Nonrepudiation Draft*, PhD Thesis, Economics University of Peiraeus, Athens, Greece.

Lagou, P., & Chondrokoukis, G. P. (2009). Survey on non repudiation: Digital signatures vs. biometrics. *Information Security Journal*, 18(5), 257–266.

Mahadevan, B., & Venkatesh, N. S. (2000). Building on-line trust for business to business e commerce. IT Asia Millenium Conference, Bombay, India, November 29–30. Retrieved from http://onemvweb.com/sources/sources/building_online_trust_ecommerce.pdf

Onieva, J. A., Zhou, J., Lopez, J., & Carbonell, M. (2004). Agent-mediated non-repudiation protocols. Retrieved from http://www.nics.uma.es/sites/default/files/ECRA04.pdf

Ou, C.-M., & Ou, C.-M. (2008). Non-repudiation mechanism of agent-based mobile payment systems perspectives on wireless PKI. *Journal of Universal Computer Science*, 14(14). Retrieved from http://www.jucs.org/jucs_14_14/non_repudiation_mechanism_of/jucs_14_14_2309_2328_ou.pdf

Perez, A. (2000). Ten risks of PKI, response. Retrieved from http://homepage.mac.com/aramperez/responsetenrisks.html

Panagiota Lagou is a Ph.D. Student in the Department of Industrial Management, University of Piraeus. She has a Degree in Economics from the

Department of Economics, Athens University of Economics and Business, and a Master's 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. from the Department of Economics, University of Piraeus, and B.Sc. in Business Administration from 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 30 European Projects in the area of Small Medium Sized Enterprises, Strategic Planning for Business, Human Computer Interaction, Interfaces Design, Industrial Management, E-Commerce, etc. He has published in several journals over 40 publications in the field of Operational Research, Decision Support and Expert Systems and Business Analysis. He was Chairman in Public Sector Enterprises.