Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems

Aleksandar Valjarevic,
Department of Computer Science
University of Pretoria,
Pretoria, South Africa
alexander@vlatacom.com

HS Venter,
Department of Computer Science
University of Pretoria,
Pretoria, South Africa
hventer@cs.up.ac.za

Abstract—

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates [18]. PKI systems are today one of the most accepted and used technologies to enable successful implementation of information systems security services such as authentication and confidentiality.

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime [2][3]. A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. In fact, there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs. Digital forensic readiness enables an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation [7].

The problem that this paper addresses is that there is no Digital Forensic Readiness Framework for PKI systems, thus not enabling an implementation of Digital Forensic Readiness measures to PKI systems. This paper focuses on defining the basic postulates of a Digital Forensic Readiness Framework for PKI systems. The authors investigate a model that can be proposed to accomplish this and also certain policies, guidelines and procedures which can be followed. When proposing the framework the authors take into account requirements for preserving or improving information security and not to interfere with the existing PKI systems' business processes.

Keywords: information systems security, Public Key Infrastructure, Digital Forensic Readiness.

I. INTRODUCTION

Over the past few years, digital forensics has risen to the fore as an increasingly important method of identifying and prosecuting computer criminals and implementing investigations relating to computer crime, data corruption, data recovery, system crashes and all other incidents requiring investigation as defined by policies of the information system owner [1].

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates [18]. PKI systems today present one of the most accepted and used technologies to enable successful implementation of information systems security services such as authentication and confidentiality. These systems are of extreme importance for e-Government implementations, e-Commerce implementations, electronic documents solutions, electronic transactions solutions, secure e-mail solutions and other information systems implementations that require strong authentication and encryption.

It is with this in mind that authors defined the following problem statement. The problem is that, currently, there is no Digital Forensic Readiness (DFR) Framework for PKI systems, thus not enabling an implementation of Digital Forensic Readiness measures to PKI systems.

The authors have defined the concept of a DFR Framework for PKI systems as follows. A DFR Framework for PKI systems is set of recommended concepts, values and practices that constitute the way DFR should be implemented to PKI systems. The proposed framework includes a model and set of guidelines and procedures to be followed when implementing DFR for PKI systems. The authors see the DFR model for PKI systems as schematic representation of the process to be followed when implementing DFR for PKI systems.

The paper is structured as follows. The first section introduces the paper and provides the problem statement. Section II gives an overview of past work on Digital Forensic Readiness and Public Key Infrastructure, setting the background for this work. The next section explains a proposed Digital Forensic Readiness Framework for Public Key Infrastructure systems. Section IV concentrates on discussing the proposed framework. The last section concludes this paper and indicates possible future work.

II. BACKGROUND

This section gives an overview of past work on Digital Forensic Readiness and Public Key Infrastructure systems. We cover basic principles and models proposed for digital forensic readiness and for PKI principles and architecture.

A. Digital Forensic Readiness

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often

Vlatacom South Africa Pty Ltd
Vlatacom d.o.o

in relation to, but not limited to, computer crime [2][3]. A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. In fact, there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs [7]. Digital forensic readiness is defined as the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation [4].

What follows is a brief overview of work relating to digital forensic readiness.

Tan [4] identified factors that affect digital forensic readiness:

- how logging is done;
- what is logged;
- Intrusion Detection Systems (IDS);
- forensic acquisition;
- evidence handling.

Yasinsac and Manzano [5] propose six categories of policies to facilitate digital forensics readiness:

- retaining information;
- planning the response;
- training;
- accelerating the investigation;
- preventing anonymous activities;
- protecting the evidence.

Wolfe-Wilson and Wolfe [6] emphasize the need for an organization to have procedures in place in order to preserve digital evidence in the event that DFI is needed.

Rowlingson [7] defines digital forensic readiness goals as:

- To gather admissible evidence legally and without interfering with business processes;
- To gather evidence targeting the potential crimes and disputes that may adversely impact an organization;
- To allow an investigation to proceed at a cost in proportion to the incident;
- To minimize interruption to the business from any investigation;
- To ensure that evidence makes a positive impact on the outcome of any legal action.

Rowlingson [7] also defines key activities in implementation of digital forensic readiness:

- Define the business scenarios that require digital evidence;
- Identify available sources and different types of potential evidence;
- Determine the evidence collection requirement;
- Establish a capability for securely gathering legally admissible evidence to meet the requirement;
- Establish a policy for secure storage and handling of potential evidence;
- Ensure monitoring is targeted to detect and deter major incidents;
- Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
- Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
- Document an evidence-based case describing the incident and its impact;
- Ensure legal review to facilitate action in response to the incident.

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [11], the need for a standard framework for digital forensics has been acknowledged by the information security society.

A framework for digital forensics needs to be flexible enough so that it can support future technologies and different types of incidents. Therefore, it needs to be simple and abstract. On the other hand, if it is too simple and abstract then it is difficult to create tool requirements and test procedures for each phase [12].

There are several works presenting digital forensic models, which include readiness as a phase. These are briefly mentioned below. Note that in this paper, however, the words *framework* and *model* are used with the following relation. The framework can contain a model, but also other components proposed by this paper, such as policies, guidelines and procedures.

Carrier and Spafford [8] proposed a digital investigation process model, which has 17 phases, divided in five groups, one group being readiness phases. The group contains two phases: operation readiness phase and infrastructure readiness phase. .

Mandia, Prosise, and Pepe [9] also proposed a digital investigation process that includes a readiness phase, known as the pre-incident preparation phase.

Beebe and Clark [10] proposed the Hierarchical, Objectives-Based Framework for the Digital Investigations Process, which includes a preparation phase. Beebe and Clark equate preparation phase with achieving digital forensic readiness. They also gave a comparison of different digital forensic models, where only the models of Carrier and Spafford [8] and Mandia, Prosise and Pepe [9] included a preparation phase. Preparation phases mentioned here include activities that are required to achieve digital forensic readiness.

Although Rowlingson [8] has not defined a digital forensic readiness model, based on his work such model can also be defined.

The next subsection gives a brief overview of PKI principles.

B. *Public Key Infrastructure*

The major strength of public key encryption is its ability to facilitate communication between parties previously unknown to each other. This is made possible by the PKI hierarchy of trust relationships [13].

Public key cryptography (also called “two key” or “asymmetric” cryptography) was invented by Diffie and Hellmann 1976 [14]. Unlike secret key (also called “symmetric”) cryptography, in which the same key is shared between two parties, pairs of corresponding private and public keys for each user allow the unique realization of some operations.

PKI derives its name from Public Key Cryptography. However, in practice, PKI represents the integration of public key cryptography, which is used for key management, digital signatures and rarely for encryption (i.e. for encryption of e-mails), and symmetric key cryptography, which is used only for encryption. (Note: secret keys used for encryption are exchanged using public key cryptography.)

The basic PKI architecture model has remained largely unchanged since it was first published in the original Internet Certificate and Certificate Revocation List (CRL) Profile [RFC2459][16]. The latest model is reflected in the most recent version of the Internet Certificate and Certificate Revocation List (CRL) Profile [RFC5280] [17].

Following is a simplified view of the architectural model for the Public-Key Infrastructure as specified in the X.509 digital certificate specifications standard [17]. The components in this model are:

- End Entity: user of PKI certificates and/or end user system that is the subject of a certificate;
- CA: A Certification Authority is an entity which issues digital certificates and can perform digital certificate management functions;
- RA: Registration Authority, i.e. an optional system to which a CA delegates certain management functions;
- CRL issuer: a system that generates and signs Certificate Revocation Lists (CRLs). CRLs contain data about all digital certificates that have been revoked due to loss, expiry etc. by a CA. These lists are published periodically and are used to verify the validity of digital certificates;
- Repository: a system or collection of distributed systems that stores certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

As seen in Section I the authors defined the PKI systems as a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates [18].

Digital certificates provide communicating parties with the assurance that they are communicating with people who truly are who they claim to be. Digital certificates are essentially endorsed copies of an individual's public key. This prevents malicious individuals from distributing false public keys on behalf of another party and then convincing third parties that they are communicating with someone else. Digital certificates contain specific identifying information, and their construction is governed by an international standard—X.509 [13]. Digital certificates are used for the purpose of digital signing mechanisms and encryption mechanisms.

The next section presents a proposal for a Digital Forensic Readiness Framework for PKI systems.

III. PROPOSING A DIGITAL FORENSIC READINESS FRAMEWORK FOR PKI SYSTEMS

Recall the problem statement, i.e. there is currently no Digital Forensic Readiness Framework for PKI systems. Therefore, no implementation of Digital Forensic Readiness (DFR) measures to PKI systems exists to the best of the authors' knowledge. The authors are proposing a framework which is explained in more detail in this section. This proposed framework should give guidance for the implementation of DFR for PKI systems.

First the authors define aims and a general policy for the proposed framework. Thereafter a DFR model for PKI systems is given.

A. Aims and policy

The authors have defined the following aims for a DFR Framework for PKI systems based on previous work [4] [5] [6] [7] [8] [9] [10] [11]:

1. To maximize the potential use of digital evidence;
2. To minimize the costs of investigations incurred either directly onto the PKI system, or related to PKI system's services;
3. To minimize interference with and prevent interruption of PKI systems' business processes;
4. To preserve or improve the current level of information systems security of PKI systems.

The authors have added the last aim above, which has not been identified in previous work: The authors firmly believe that this aim has to be taken into account when implementing DFR measures and even more when proposing this framework. It is not viable to only concentrate on efficiency of the investigation (aims 1 and 2) and non-interference with business processes (aim 3), because having only the first three aims could still leave room for flaws in the overall information security of an enterprise. An example of such a flaw could involve the following. Suppose an enterprise keeps dedicated access control logs. Making image copies of these logs in the event of a digital forensic investigation is crucial for the investigation; however, creating the image copies is often a time-consuming process. If the imaging is done on off-peak times, such as after hours, it would not interfere with the business processes of the enterprise. On the contrary, if appropriate information security measures are not applied to the logs themselves, such as access control and encryption during transmission, the logs can be exposed and in that way leave the logs vulnerable to compromise, leading to possible compromise of the entire information system.

It is therefore necessary to take a more holistic approach by applying DFR to information systems security. The authors believe that DFR should be a built-in security feature and not merely an add-on.

These aims are to be achieved through defining a relevant framework by employing a relevant model, policies, guidelines and procedures. The authors firstly derive a policy that must be conformed to when implementing a DFR framework, based on aims the authors have. The following is the definition of the policy.

The policy for achieving a DFR framework within PKI systems is to maximize the potential of using digital evidence connected to a PKI system, while minimizing costs of investigations. The incident initiating the investigation can occur within the PKI system or outside of the PKI system. In the latter case, however, the incident has to be related to the PKI system's services. Interference with or interruption of the PKI system's business processes is not allowed while preserving or improving the current level of information systems security over the PKI system as a whole.

B. Model

Note, once more, that in this paper the words *framework* and *model* are used with the following meaning. The framework can contain a model, but also other components proposed by this paper, such as policies, guidelines and procedures.

The authors have defined a model for the implementation of DFR in PKI systems. The model has following phases:

1. Scenario definition
   (*Scenario phase*);
2. Identification of possible sources of evidence
   (*Sources phase*);
3. Defining procedures for pre-incident collection, storage and manipulation with data representing possible evidence

(*Pre-incident collection phase*);

4. Defining procedures for pre-incident analyses of data representing possible evidence (*Pre-incident analyses phase*);
5. Defining procedures for incident (*Incident detection phase*);
6. Defining procedures for post-incident collection, storage and manipulation with data representing possible evidence (*Post-incident collection phase*);
7. Defining procedures for post-incident analyses of data representing possible evidence (*Post-incident analyses phase*);
8. Defining PKI system architecture (*Architecture-defining phase*);
9. Implementing defined procedures and PKI system architecture (*Implementation phase*);
10. Assessment of digital forensic readiness implementation (*Assessment phase*).

An illustration bellow depicts the model followed by more detailed discussions of each phase in the proposed model.

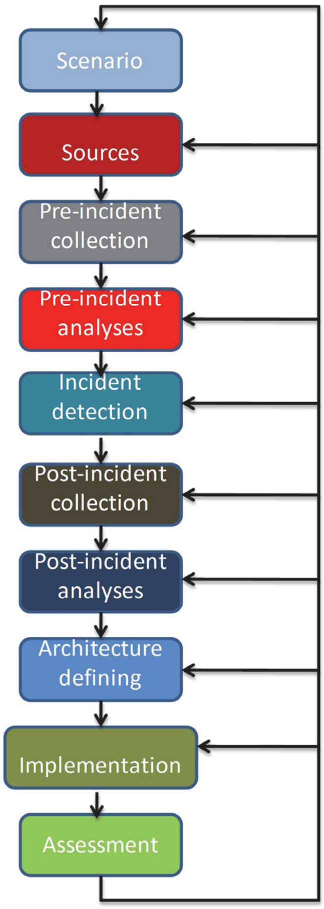

Figure 1: Digital forensic readiness model for PKI systems

As it can be seen from Figure 1, the defined model is iterative, where after the *Assessment* phase one can go back to any of the previous phases.

Inputs and outputs to each of the phases will be defined in the *Model phases* subsection.

This model can be applied for digital forensic readiness for any information system, not necessarily for PKI systems only, as it is generic enough.

In the *Model phases* subsection the authors explain each of the model phases in more detail. The authors also provide guidelines and recommended procedures for applying this model within PKI systems.

1) Model phases

a) Scenario phase

In this phase one should examine all scenarios of when digital evidence might be required.

Input to this phase includes all information regarding PKI system architecture, technology used (hardware and software), policies, procedures and business processes. The input must also include the policy stated earlier for the DFR framework for PKI systems.

The output of this phase includes the defined scenarios.

As a guideline, the authors recommend including at least the following two high-level scenarios when implementing DFR for PKI systems:

- Internal incident:
  An internal incident is any incident that occurs, that would potentially require the gathering of digital evidence within the PKI system. An example for this is unauthorized access to the PKI system.
- External incident:
  An external incident is any incident involving the PKI system's services, however, the incident occurs outside of PKI software system. An example of an external incident is when a stolen identity card containing PKI material, i.e. digital certificate and keys, are used for unauthorized access to an information system. If the card holder has reported the stolen card, the PKI system would have published revocation of the digital certificate on the card in Certificate Revocation List (CRL). This CRL, however, could later be used as digital evidence during a potential investigation of the stolen card, in order to prove innocence of the legitimate card holder. It should be clear from this example that the incident involved the use of PKI services, but the PKI system itself was not compromised by the incident.

The authors also recommend that a proper risk assessment is performed during this phase for each scenario separately. A risk assessment would enable one to better identify all possible threats, vulnerabilities and related scenarios that would expose the information asset. Based on the assessed risk from certain threats/vulnerabilities/scenarios, one can, in later phases, better decide on the needed measures to achieve DFR, taking into account the risk level and the costs and benefits of possible measures to reduce the identified risk.

b) Sources phase

In this phase one should identify all possible sources of evidence within a PKI system.

Input to this phase are all information regarding the PKI system architecture, technology used (hardware and software), policies, procedures and business processes in the same way as defined in the previous phase. Input must also include the policy of the DFR framework for PKI systems.

The output of this phase is the defined sources.

As a guideline, the authors recommend to analyze the possible use of at least the following sources when implementing DFR for PKI systems:

- volatile data;
- device images;
- log files;
- digital certificate life-cycle logs;
- access related logs;
- user life-cycle related logs;
- configuration files;
- certificates;
- Certificate Revocation Lists;
- PKI service-related logs;
- hardware security modules (HSMs).[1]

Some of the identified possible sources as listed above might not be available. For example access related logging is not introduced within PKI system, which would mean that access related logs are not available as a source of data. In that case measures should be explored to make identified source available, i.e. introducing dedicated access-related logging.

As a guideline, the authors recommend the following when implementing DFR for PKI systems:

- There should exist separate log files relating to access (log-in, access to all files);
- There should exist separate user life-cycle related logs, that should include all data related to the life-cycle of users (including OS users, application users, PKI services users);
- There should exist separate PKI services-related logs, which would be organized in such a way that one specific log consists of all data relating to one specific certificate (certificate life-cycle, CRL lists containing this certificate, life-cycle of the user that is the owner of the certificate).

c) Pre-incident collection phase

In this phase one should define procedures for pre-incident collection, storage and manipulation of data representing possible evidence.

The input to this phase includes all information regarding the PKI system architecture, technology used (hardware and software), policies, procedures and business processes, in the same way as defined in the previous phase. The input must also include the policy of the DFR framework for Public Key Infrastructure PKI systems.

The output of this phase includes the defined procedures for pre-incident collection, storage and manipulation of data representing possible evidence.

In the previous phase the authors have recommended the analysis of some data sources. In this phase, however, the authors recommend how data (possible evidence) from these sources should be collected. As a guideline the authors recommend the following procedures, regarding data collection, to be used when implementing DFR for PKI systems:

- Volatile data to be collected periodically and stored at central repository;
- Device images to be collected periodically and stored at local repository if PKI architecture is decentralized, otherwise to be stored at central repository;
- Log files to be collected periodically and stored at central repository;
- Digital certificate life-cycle logs to be collected periodically and stored at central repository;
- Access related logs to be collected periodically and stored at central repository;
- User life-cycle logs to be collected periodically and stored at central repository;
- Configuration files to be collected periodically and stored at central repository;
- Certificates to be collected periodically and stored at central repository;
- Certificate Revocation Lists to be collected periodically and stored at central repository;
- PKI Service related logs to be collected periodically and stored at central repository.

Note that the collection period is to be determined based on risk assessment. Also note that the collection, storage and manipulation of data have to conform to digital forensic principles in order to preserve the chain of evidence. Lastly, note that the retention period of data is to be determined based on two factors:

- risk assessment;
- previous experience, regarding incident detection, data quantities, network capacity and all other matters that could influence cost or efficiency of this phase.

d) Pre-incident analyses phase

In this phase one should define procedures for pre-incident analyses of data representing possible evidence.

The input to this phase includes the sources as defined in the *Sources* phase as well as the scenarios as defined in the *Scenario* phase. The input must also include the policy of the DFR framework for PKI systems.

The output of this phase includes the defined procedures for pre-incident analyses of the data that represent possible evidence.

As the task of data analyses is outside the scope of the functionalities of PKI systems, the authors recommend that this phase defines a practical interface between the PKI system and a *monitoring system,* which would analyze data in order to detect incidents. The monitoring system can be a custom system that is specialized for this purpose. It can also be any one of the following systems: Intrusion

[1] HSM is a secure cryptoprocessor with funcionalities of managing digital keys and accelerating cryptoprocesses. HSMs provide both logical and physical protection of these materials from non-authorized use and potential adversaries. In short, they protect high-value cryptographic keys [15].

Prevention Systems, Intrusion Detection Systems, Change Tracking Systems, and Log Processing Systems etc.

e) Incident detection phase

In this phase one should define the procedure of how an incident is detected.

The input to this phase includes all information regarding the PKI system architecture, technology used (hardware and software), policies, procedures and business processes, similar to the procedures defined in both of the *Pre-incident* phases listed before. Further input must also include the policy of the DFR framework for PKI systems.

The output of this phase includes the defined procedures to detect an incident.

As the task of data analyses is outside the scope of the functionalities of PKI systems, the authors recommend that this phase defines a practical interface between the PKI system and a *monitoring system,* which would analyze data in order to detect incidents. The monitoring system can be a custom system that is specialized for this purpose. It can also be any one of the following systems: Intrusion Prevention Systems, Intrusion Detection Systems, Change Tracking Systems, and Log Processing Systems etc.

f) Post-incident collection phase

In this phase one should define procedures for post-incident collection, storage and manipulation with data representing possible evidence.

Input to this phase are all information regarding PKI system architecture, used technology (hardware and software), policies, procedures and business processes, as same as sources defined in *Sources* phase and results from *Incident detection* phase. Input also must include the policy of Digital Forensic Readiness framework for Public Key Infrastructure systems.

Output of this phase is defined procedures for post-incident collection, storage and manipulation with data representing possible evidence.

In the sources phase above the authors have recommended analyzing of some data sources. In the post-incident collection phase, however, the authors recommend how data (possible evidence) from these sources should be collected. As a guideline, the authors recommend the following procedures, regarding data collection, to be used when implementing DFR for PKI systems:

- Volatile data related to the incident to be stored at dedicated central repository for this incident;
- Device images related to the incident to be stored at dedicated central repository for this incident;
- Log files related to the incident to be stored at dedicated central repository for this incident;
- Digital certificate life-cycle logs related to the incident to be stored at dedicated central repository for this incident;
- Access related logs related to the incident to be stored at dedicated central repository for this incident;
- User life-cycle logs related to the incident to be stored at dedicated central repository for this incident;
- Configuration files related to the incident to be stored at dedicated central repository for this incident;
- Certificates related to the incident to be stored at dedicated central repository for this incident;
- Certificate Revocation Lists related to the incident to be stored at dedicated central repository for this incident;
- PKI Service related logs, related to the incident to be stored at dedicated central repository for this incident.

Note that the collection of the data is to be performed when incident is detected.
Also note that all previously collected data related to the incident is to be stored at dedicated central repository.
Lastly note: Retention period of data to be determined based on information security risk assessment, as same as based on previous experience with incident detection, data quantities, network capacity and all other matters that could influence cost or efficiency of this phase.

g) Post-incident analyses phase

In this phase one should define procedures for post-incident analyses of data representing possible evidence.

Input to this phase is sources defined in *Sources* phase and scenarios defined in *Scenario* phase. Input also must include the policy of Digital Forensic Readiness framework for Public Key Infrastructure systems.

Output of this phase is defined procedures for post-incident analyses of data representing possible evidence.

As guideline the authors recommend following procedure to be used, when implementing Digital Forensic Readiness for PKI systems:
During this phase data collected in dedicated central repository, during the previous phase should be analyzed. Based on information about the incident (time of incident, type of incident, affected entities, etc.) and collected data in dedicated central repository initial presentation of data should be prepared, to contain (not exclusively):

- Time-line of events related to the incident (access to the system, application actions, PKI services actions);
- Relation of users related to the incident;
- Time-line of all recorded actions of users related to the incident;
- All noted irregularities, in addition to those detected within the incident (hardware, software).

h) Architecture-defining phase

In this phase one should define PKI system architecture, while taking into account results of all previous phases for post-incident analyses of data representing possible evidence.

Input to this phase is results from all previous phases. Input also must include the policy of Digital Forensic Readiness framework for Public Key Infrastructure systems.

Output of this phase is defined PKI system architecture.

As guideline the authors recommend analyzing at least following matters, when implementing Digital Forensic Readiness for PKI systems.

1. Whether architecture should be centralized or decentralized, or combined?

Holistic approach must be taken, which would include evaluating all benefits of proposed architecture, from Digital Forensic Readiness Framework aims fulfillment to PKI system business process efficiency. For example for environment where PKI services are to be provided to large number of end-entities and where those entities are geographically or logically sparsely distributed, from PKI system business process efficiency standpoint it is better to have distributed PKI architecture. On the other side with distributed architecture issue of network capacity and network costs appears in relation to collection, storage and manipulation with data identified in Pre-*incident collection* and *Post-incident collection* phases. These two standpoints must be included and evaluated when making final decision on PKI architecture.

2. Whether functions should be off-loaded from CA?

This includes functions of registration, CRL list publishing and other functions that can be off-loaded as defined by PKIX architecture model. Holistic approach must be taken, which would include evaluating all benefits of proposed architecture, from Digital Forensic Readiness Framework aims fulfillment to PKI system business process efficiency. For example for environment where PKI services are to be provided to large number of end-entities, from PKI system business process efficiency standpoint it is better to have as much functions as possible off-loaded from CA. This is also true from information security standpoint, when one can isolate CA to great extent in order to be more secure. On the other side with off-loaded functions, the authors have more entities within PKI architecture and more data to be collected and analyzed, so issue of network capacity, network costs and processing costs appears in relation to collection, storage and manipulation with data identified in Pre-*incident collection* and *Post-incident collection* phase. These standpoints must be included and evaluated when making final decision on PKI architecture.

i) Implementation phase

In this phase one implements results of all previous phases.

Input to this phase is all information regarding PKI system architecture, used technology (hardware and software), policies, procedures and results from all previous phases. Input also must include the policy of Digital Forensic Readiness framework for Public Key Infrastructure systems.

Output of this phase is implemented Digital Forensic Readiness for PKI system.

As guideline the authors recommend that during this phase, one takes into account role of people in the PKI system. People represent end-entities, but also custodians and owners of the system. It is important that all procedures include relevant information for people involved with PKI system. It is important to perform required training and awareness sessions with all people involved with PKI system.

In addition to this needed technical capabilities are to be developed during this phase.

The authors also recommend that during this phase all outputs from all phases are documented in detail.

j) Assessment phase

In this phase one performs an assessment of implemented Digital Forensic Readiness for PKI system and compares it to Digital Forensic Readiness Framework for PKI system, its aims and policy.

Input to this phase are all information regarding PKI system architecture, used technology (hardware and software), policies, procedures and business processes, as same as results from all previous phases.

Output of this phase is results of assessment of implemented Digital Forensic Readiness for PKI system, which should include recommendations for changes in one or more of the previous phases.

As guideline the authors recommend analyzing following matters, when implementing Digital Forensic Readiness for PKI systems. All procedures, measures and architectures defined when implementing this model have to go through legal revision during *Assessment* phase in order to ensure admissibility of possible evidence in court.

The next subsection gives additional recommendations that are related to identity issues. These recommendations form an integral part of the proposed framework.

C. Identity related recommendations

The authors highly recommend the following in regards to the architecture of PKI systems:

- There should be an interface to an automated biometric identification system;
- There should be an interface to an identity management system;
- Verification of identity when accessing the PKI system at all levels (OS, application, PKI services) should be performed via multi-factor authentication, for example requiring biometrics, a digital certificate (except when a person applies for digital certificate) and a password.

An interface with an automated biometric identification system should ensure accurate verification of the identity of any person requesting issuance of a digital certificate from a PKI system. This can be done during the registration process, while a certification authority (or trusted third party) is verifying the identity of an applicant for a digital certificate.

The interface with the identity management system should ensure that there is proper management of identities within the PKI system at all levels of access (OS, application, PKI services). One physical person should have one identity (not meaning one role) within the PKI system.

The identity management system and measures for identity verification should be used to set up access controls based on user roles in the system. Information within the system should be classified in order to ensure that confidentiality is preserved. Strict access controls should exist for all information which contains personal data in order to achieve desired level of privacy of the users.

These measures would ensure successful identification of physical individuals, based on information from the PKI system and systems interfaced with the PKI system. This would mean that the PKI system has higher level of digital forensics readiness.

The following section focuses on discussing the proposed framework, by focusing on comparisons of our proposed framework to existing digital forensic investigation frameworks and models.

IV. DISCUSSION

The proposed model has a wider scope than the scope of digital forensic readiness, which previous models have proposed. The wider scope is due to differently defined aims and it is manifested through the following additional phases as defined in our model: data-analyses phase, post-incident phase, architecture defining phase and assessment phase.

The phases in the proposed model are well defined in terms of scope and functions. The proposed procedures and guidelines include all matters covered in previous models and also analyze matters that were out of scope of previous models, such as post-incident collection, post-incident analyses and defining architecture of the target information system (in this case the PKI system).

Also, it is to be noted that the proposed framework gives specific guidelines and proposed procedures relating to PKI systems specifically, i.e. interfacing to automatic biometric recognition systems and identity management systems, and collection of data from HSMs.

In addition, the framework provides recommendation in relation to interfacing with automated biometric identification systems and identity management systems. The authors also give recommendations regarding modalities for access control. The aim of this is to enable successful identification of physical individuals. This identification would be based on information from the PKI system and systems that interface with the PKI system. This would ultimately result in incorporating digital forensic readiness into the PKI system.

V. CONCLUSION

Let us revisit the problem statement: there exists no Digital Forensic Readiness Framework for PKI systems. In order to address this problem, the authors defined aims for proposing a Digital Forensic Readiness Framework for PKI systems. The aims have been defined based on previous work while the authors added one additional aim, which was not identified in previous work, namely the aim to preserve or improve the current level of information systems security of PKI systems.

This paper has defined the basic postulates of a Digital Forensic Readiness Framework for PKI systems. Based on the defined aims, the authors proposed a framework. The frameworks core part is the DFR model for PKI systems. The authors also proposed procedures and gave a series of recommendations in regards of implementation of this model.

The proposed framework will enable researchers and practitioners to develop PKI system solutions which would have digital forensic readiness as a built-in feature, not simply as an add-on.

Claims made in this paper are to be verified through an appropriate prototype as future work. The scope of the prototype is to apply the proposed framework to a fully functional PKI system and measure its conformance to the Digital Forensic Readiness Framework for PKI systems, before and after the implementation. More future work could also include the development of more procedures to be included as guidelines for the framework implementation.

REFERENCES

[1] Michael Kohn, JHP Eloff and MS Olivier (2006); ”Framework for a Digital Forensic Investigation”; In Proceedings of ISSA 2006.

[2] M Reith, C Carr, G Gunsch (2002); “An examination of digital forensic models”; International Journal of Digital Evidence.

[3] B Carrier (2001); “Defining digital forensic examination and analysis tools”; Digital Research Workshop II.

[4] Tan, J. (2001); ”Forensic readiness”; Technical. Cambridge USA: @stake, Inc.

[5] Yasinsac, A. and Manzano, Y. (2001); “Policies to Enhance Computer and Network Forensics”; Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.

[6] Wolfe-Wilson, J. and Wolfe, H.B. (2003); “Management strategies for implementing forensic security measures”; Information Security Technical Report Volume 8, Issue 2.

[7] R Rowlingson (2004); “A Ten Step Process for Forensic Readiness”; International Journal of Digital Evidence.

[8] Carrier B. and Spafford E. (2003); “Getting Physical with the Digital Investigation Process”; International Journal of Digital Evidence Vol 2, 2.

[9] Mandia, Kevin, Prosise, Chris, and Pepe (2003); “Incident Response & Computer Forensics”; (Second Ed.) McGraw-Hill/Osborne, Emeryville.

[10] Nicole Lang Beebe, Jan Guynes Clark (2005); ”A Hierarchical, Objectives-Based Framework for the Digital Investigations Process”; Digital Investigation 2(2) 2005.

[11] Gary Palmer (2001); “A Road Map for Digital Forensic Research”; Technical Report DTR-T001-01, DFRWS, November 2001; Report From the First Digital Forensic Research Workshop (DFRWS).

[12] Carrier B. and Spafford E. (2005); “An Event-Based Digital Forensic Investigation Framework”; Digital Investigation 2(2) 2005.

[13] James Michael Stewart, Ed Tittel, Mike Chapple (2008); ”Certified Information Systems Security Professional Study Guide Fourth Edition”; Wiley Publishing, Inc., Indianapolis, Indiana.

[14] W. Diffie, M. Hellman (1976); “New Directions in Cryptography”; IEEE Transactions on Information Theory, Vol. 22, No. 6.

[15] http://en.wikipedia.org/wiki/Hardware_Security_Module.

[16] R. Housley, W. Ford, W. Polk, D. Solo (1999); “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”; The Internet Society.

[17] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk (2008);“Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ”; The Internet Society.

[18] M. Toorani, A.A.B. Shirazi (2008); “LPKI- a Lightweight Public Key Infrastructure for the mobile environments”; Proceedings of the 11th IEEE International Conference on Communication Systems.