



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Denkeleers • Leading Minds • Dikgopolo tša Dihalefi

Towards Digital Forensic Readiness Framework for Public Key Infrastructure Systems

Authors:

Aleksandar Valjarevic

HS Venter

**ICSA Research Group
Department of Computer Science
School of Information Technology
University of Pretoria**

Introduction

- Definition of Digital Forensic Readiness:

Digital Forensic Readiness is defined as ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation.

- Definition of Public Key Infrastructure:

The Public Key Infrastructure is a set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke digital certificates.

- Problem statement:

The Problem is that currently there is no Digital Forensic Readiness (DFR) Framework for Public Key infrastructure (PKI) Systems, thus not enabling full and most efficient implementation of DFR measures to PKI systems and organizations and systems that utilize PKI systems.



Introduction

- DFR Framework for PKI Systems- concept:

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 Proposed Framework

- Aims

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, and
4. To preserve or improve the current level of information systems security of PKI systems.

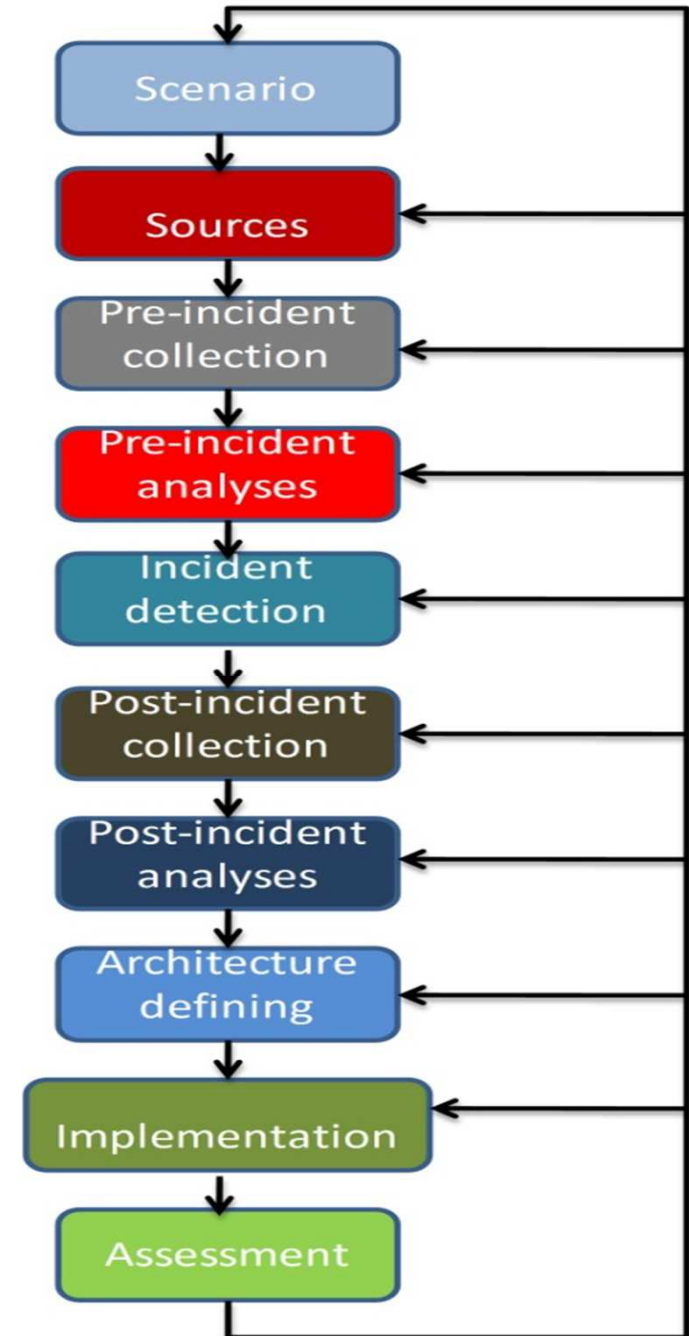
- Policy

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 is an imperative.

The Proposed Framework

- Model

- Iterative
- Pre-and post incident phases
- Holistic approach to information security
(Influencing system architecture)



The Proposed Framework

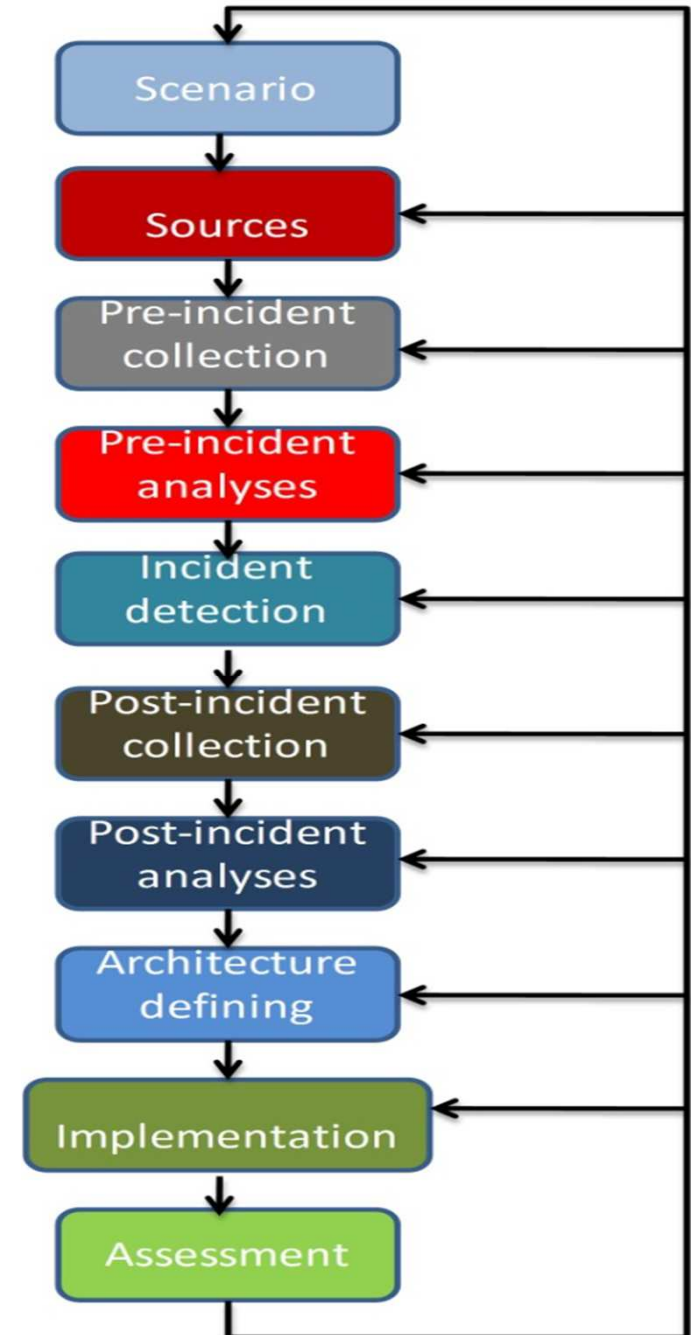
- Scenario phase

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

Inputs: all information regarding PKI system architecture, technology used (hardware and software), policies, procedures and business processes.

The output of this phase includes the defined scenarios.

Guideline:
Internal vs. External scenario
Risk assessment



The Proposed Framework

- Sources phase

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

Inputs: all information regarding PKI system architecture, technology used (hardware and software), policies, procedures and business processes + scenarios.

The output of this phase is the defined sources.

Guideline:

Possible sources:

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).

Measures should be explored to make identified source available.

The Proposed Framework

- Pre-incident collection phase

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

Inputs: all information regarding PKI system architecture, technology used (hardware and software), policies, procedures and business processes + scenarios + sources.

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

Guideline:

In this phase, the authors recommend how data (possible evidence) from sources should be collected.

Collection period is to be determined based on risk assessment.

Preserving the chain of evidence.

Retention period of data is to be determined based on two factors: risk assessment & previous experience.

The Proposed Framework

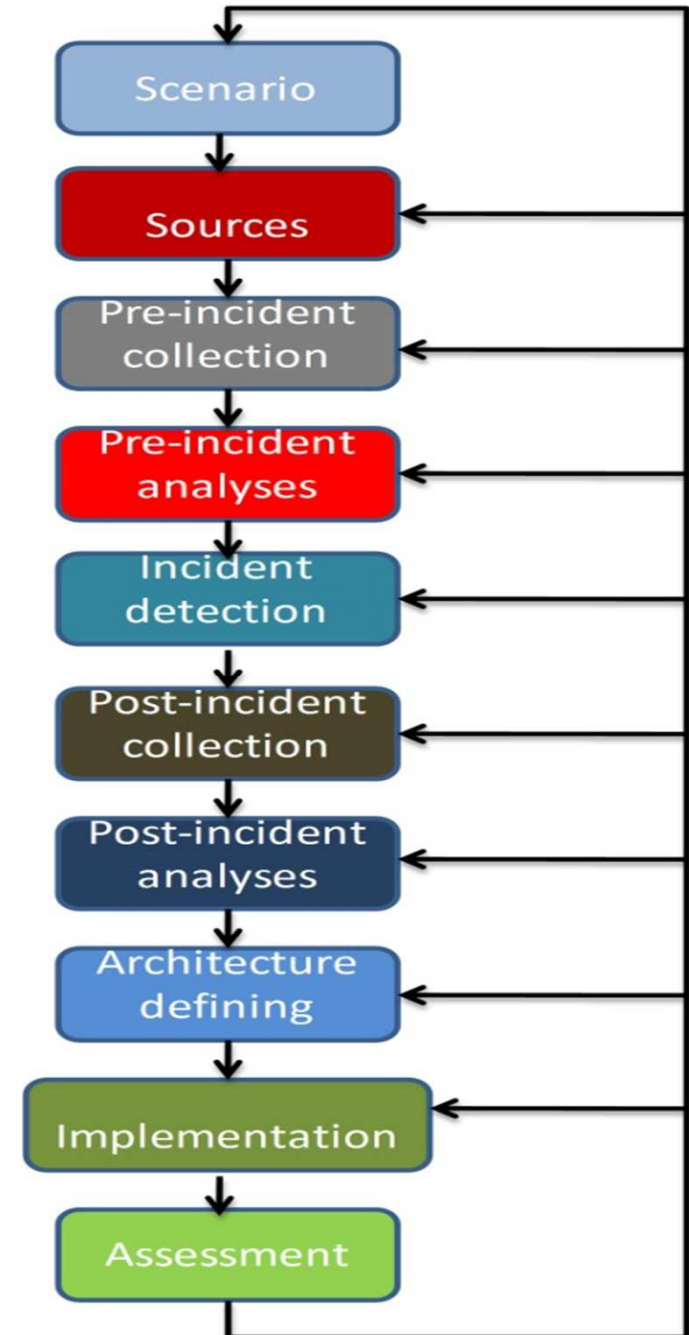
- Pre-incident analyses phase

In this phase one should define procedures for pre-incident analyses of data representing possible evidence. Aim is to detect an incident.

Inputs: Sources + Scenarios

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

This task 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* (custom system Intrusion Prevention Systems, Intrusion Detection Systems, Change Tracking Systems, and Log Processing Systems etc.)



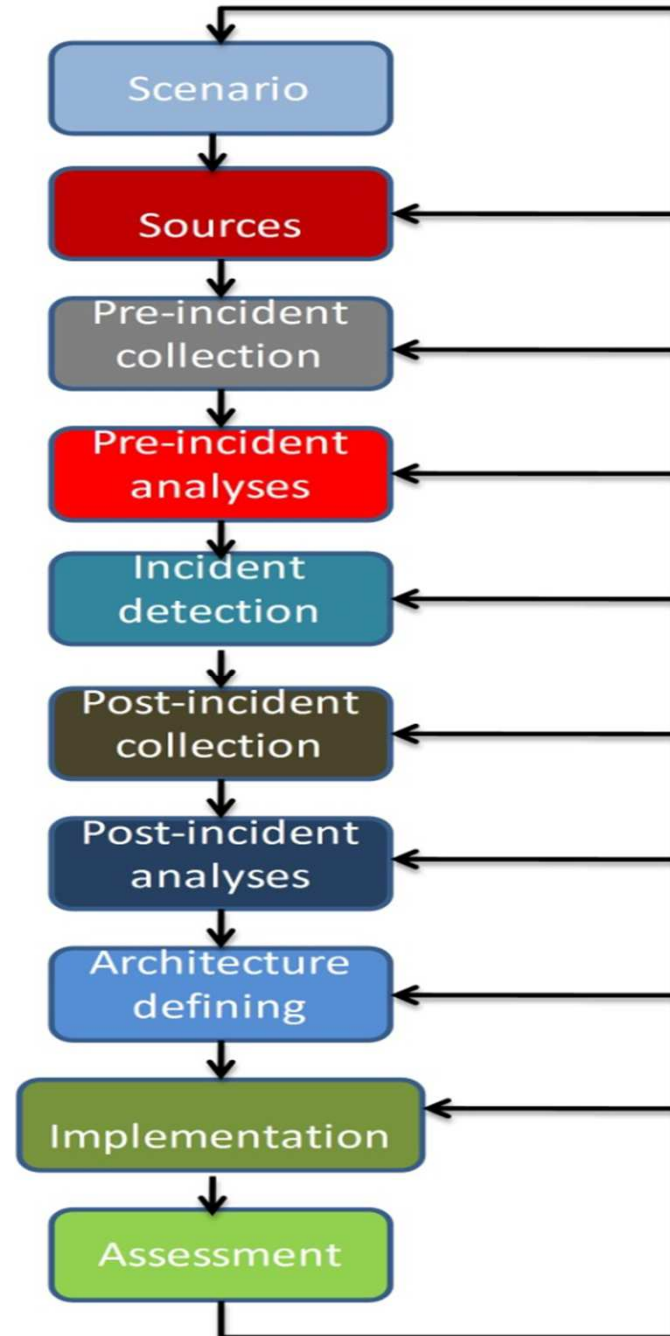
The Proposed Framework

- Incident detection phase

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

Inputs: outputs from other phases.

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



The Proposed Framework

- Post-incident collection phase

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

Inputs: all information regarding PKI system architecture, technology used (hardware and software), policies, procedures and business processes + outputs from other phases.

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

Guideline:

In this phase the authors recommend how data (possible evidence) from sources should be collected.

Relevant previously collected data related to the incident is to be stored at dedicated central repository.

The Proposed Framework

- Post-incident analyses phase

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

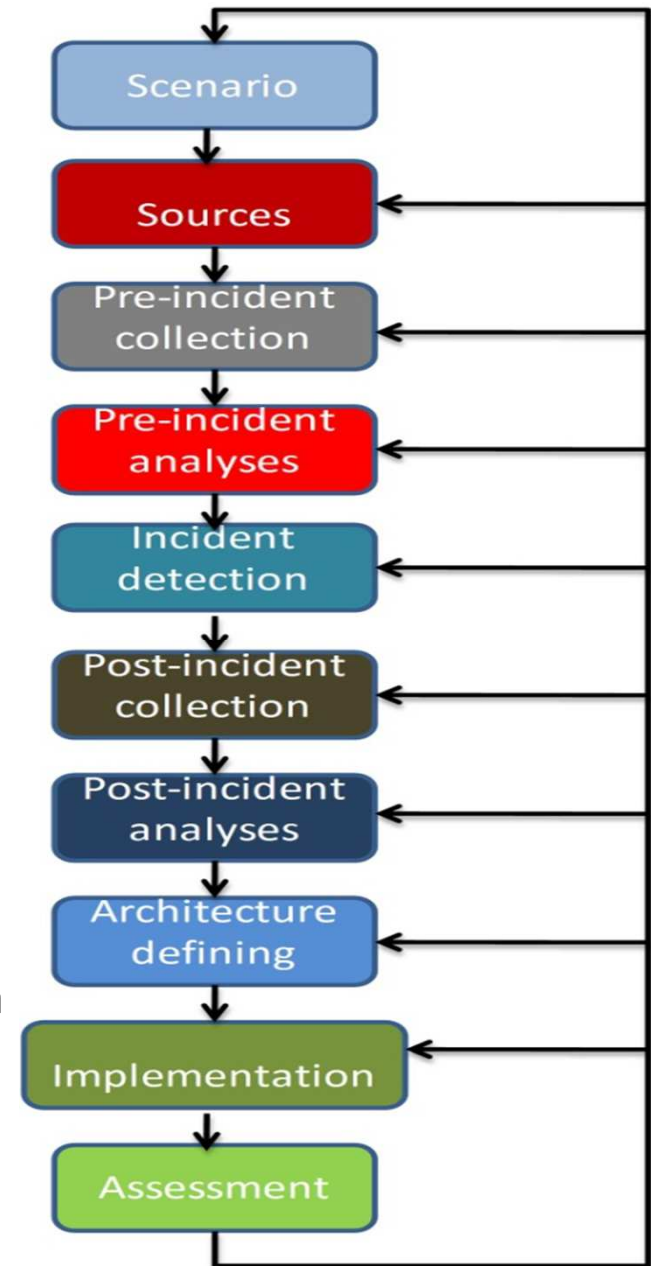
Inputs: Sources + Scenarios

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

Guideline:

Based on information about the incident and collected data initial presentation should be prepared, to contain (not exclusively):

- Time-line of events related to the incident;
- Relation of users related to the incident;
- Time-line of all recorded actions of users related to the incident;
- All noted irregularities.



The Proposed Framework

- 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.

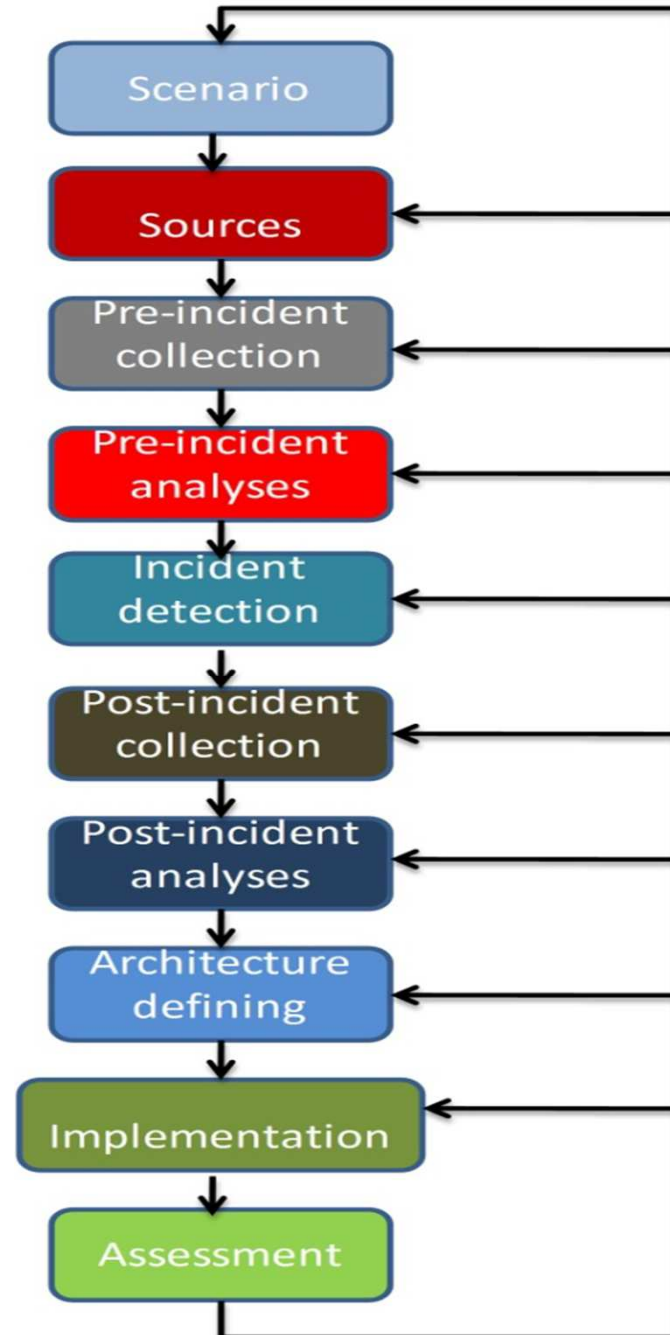
Inputs: outputs from all phases.

Output of this phase is defined PKI system architecture.

Guideline:

Analyzing at least following matters, when implementing Digital Forensic Readiness for PKI systems:

- Centralized vs. decentralized architecture;
- Offload of CA activities.



The Proposed Framework

- Implementation phase

In this phase one implements results of all previous phases.

Inputs: all information regarding PKI system architecture, used technology (hardware and software), policies, procedures and results from all previous phases.

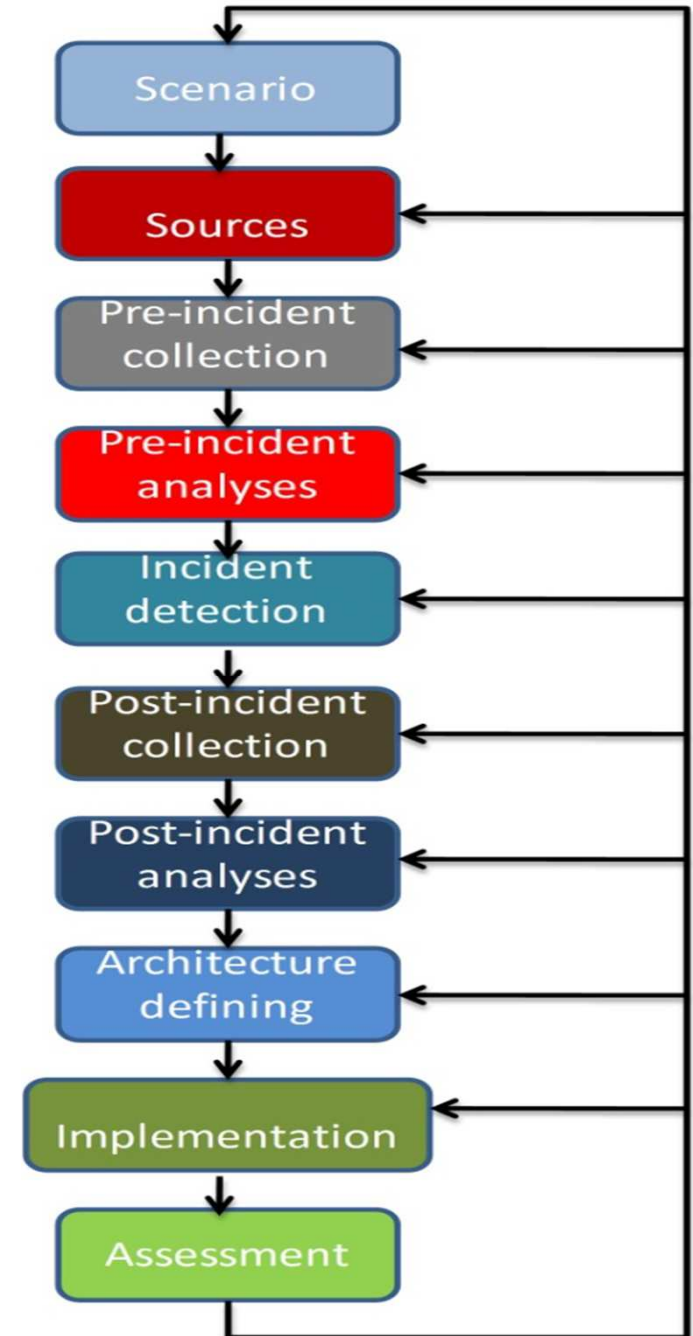
Output of this phase is implemented Digital Forensic Readiness for PKI system.

Guideline:

Takes into account role of people in the PKI system. (procedures, training, awareness)

Needed technical capabilities are to be developed during this phase.

All outputs from all phases to be documented in detail.



The Proposed Framework

- Assessment phase

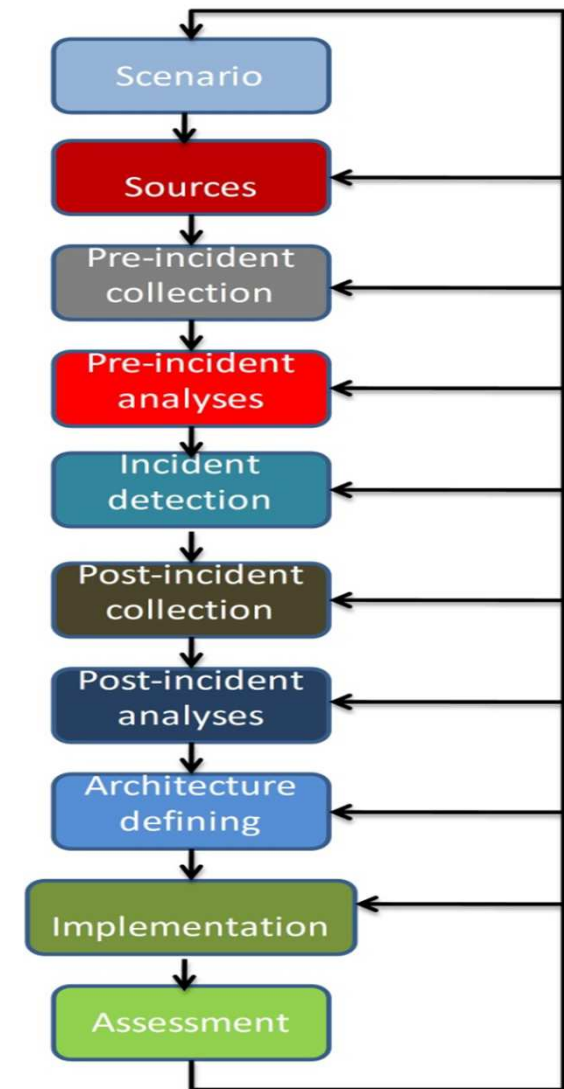
In this phase one performs an assessment of implemented Digital Forensic Readiness for PKI system and compares it to Digital Forensic Readiness Framework for PKI system, its aims and policy.

Inputs: 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.

Guideline:

All procedures, measures and architectures defined have to go through legal revision during *Assessment* phase in order to ensure admissibility of possible evidence in court.



The Proposed Framework

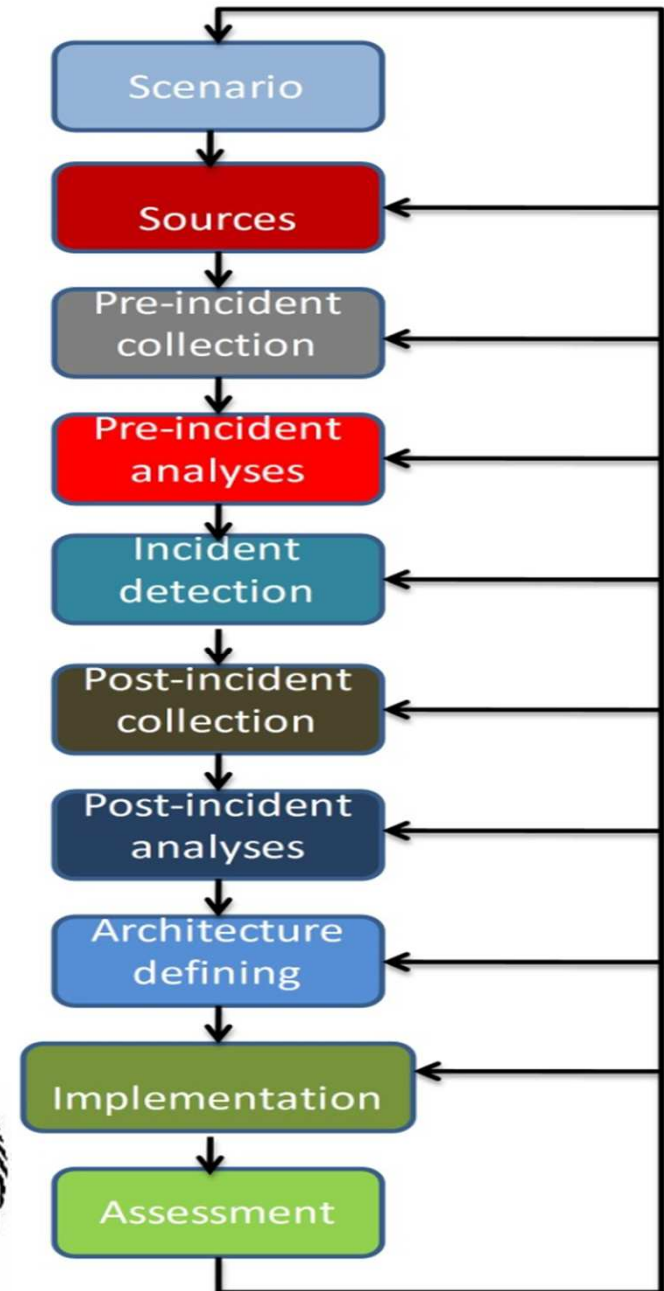
Identity related recommendations:

- 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.



Discussion

- Model comprehensiveness
- Specific guidelines and proposed procedures relating to PKI systems
- Identity related recommendations



Conclusion

- Step towards DFR Framework for PKI Systems
- Further research enabled
- Help to practitioners
- Future work:
 - Claims made in this paper are to be verified through appropriate prototype.
 - Developing more procedures to be included as guidelines for framework implementation, especially in respect of specific digital forensic measures and specific entities within PKI systems.



Thank You for Your attention.

Questions?