Incident Management Process

For The

Federal Public Key Infrastructure (FPKI) Community

Version 1.0.0

February 21, 2012

Document History

Version	Date	Revision Details
v1.0.0	2/21/12	Final based on CPWG review and comment period

Editors

Christine Abruzzi	Wendy Brown	Matt King
Jeff Jarboe	Dave Silver	

Table of Contents

Figures

Tables

1 Introduction

1.1 Background

The Federal Public Key Infrastructure (FPKI) is an interoperable public key infrastructure (PKI) supporting the federal government and promoting mutual trust between federal agencies, and between federal agencies and external PKIs. Drivers for the FPKI include the statutory mandates for electronic government, electronic signature technology, demands for improved services at lower cost, and to support federal agency business processes.

The FPKI has grown to become a core component of the broader Federal Trust Framework. Today, the FPKI is the foundation for secure e-government certificate-based transactions at unclassified levels of assurance 1 through 4[1]. There are many communities of interest participating in the FPKI. In addition, the FPKI offers a variety of capabilities to it members, including facilitating secure (trusted) physical and logical access, document sharing, and communications (a) across federal agencies, and (b) between federal agencies and outside bodies such as universities, state and local governments, commercial entities, shared service providers, and community-of–interest bridges. The FPKI Community also indirectly includes Relying Parties that trust the certificates issued by PKI domains within the FPKI, and vendors that supply the software and hardware used in FPKI Community members' PKI domains.

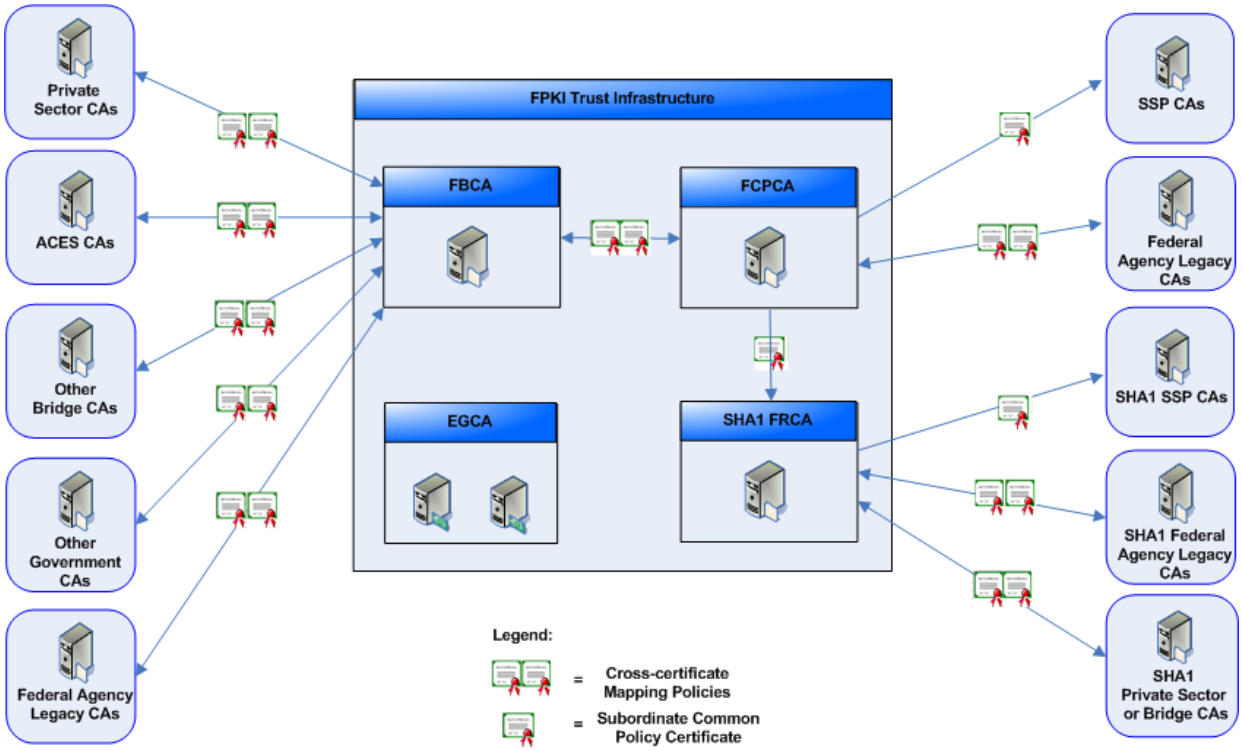
The FPKI unifies disparate PKI domains into a cohesive FPKI by creating trust paths among the participating PKI domains. The primary mechanism for unification is the FPKI Trust Infrastructure, which issues cross-certificates at specified levels of assurance within the FPKI membrane to map policies between PKI domains. The FPKI Trust Infrastructure is owned and operated by the federal government.

These established, well-defined relationships create an environment in which different organizations can trust each other's PKI credentials – the essence of the FPKI. As Figure 1 illustrates, the FPKI Trust Infrastructure is composed of the following PKI Certification Authorities (CAs):

- Federal Bridge CA (FBCA)
- Federal Common Policy Framework CA (FCPCA)
- E-Governance CAs (EGCA)
- SHA-1 Federal Root CA (SHA1 FRCA)

[1] These are the Levels of Assurance as defined by Office of Management and Budget (OMB) M-04-04.

Figure 1 FPKI Trust Infrastructure and its Affiliate CA Relationships



The FCPCA is the trust anchor for digital certificates for the PIV credentials. The FBCA is a bridge that facilitates interoperability between FPKI Community CAs. The EGCA is the source of various non-person entity (NPE) credentials such as identity provider (IdP) credentials, relying party (RP) credentials, metadata signer credentials, and backend attribute exchange (BAE) broker certificates. The SHA1 FRCA supports FPKI Community members that cannot yet support SHA-256.

Due to the complexity of the interconnected relationships within the FPKI Community, any incident that impacts one area of the community can quickly spread to impact other areas of the community (or the entire FPKI Community). Security-specific incidents threaten the FPKI and its trust relationships at various interfaces, including the systems' hardware and software, the credentials, the registration processes, and the authentication protocols. These threats include unauthorized system penetration and compromise, theft of a token (e.g., cryptographic module, password), impersonation of an individual, eavesdropping, and active attacks against authentication mechanisms. A security incident could seriously impact the assurance level provided by one or more areas of the FPKI community. The types of impacts include, but are not limited to:

- **PKI Domain CA artifacts compromised**
  - Disruption in government services and business
  - Adverse effect on individual privacy
  - Denied access to government facilities
  - Serious adverse effect on agency operations

- **Foundational Trust in question**
  - Serious consequence for public confidence
  - Private and public partners cost impact to recover
  - Disruption of RP applications and transactions
  - Denied access to official systems

- **FPKI Trust Infrastructure Breach**
  - Disruption of Entity PKI's trust chains
  - Re-establish a new Federal Root CA
  - Revocation and re-issuance of cross certificates to federal agencies and shared service providers (SSPs)
  - Chaos in electronic-government solutions until resolved

- **Authentication Assurance in jeopardy**
  - Damaged reputation, agency liability or financial loss
  - Harm to agency programs or public interests
  - Unauthorized release of sensitive information
  - Personal safety
  - Civil or criminal violations

Derived impacts may include time, effort, and cost for such things as certificate revocations, reissuance of cross-certificates, integration of new or updated commercial products, audits, and security authorization.

1.2 Purpose

This document serves as the Incident Management Process (IMP) for handling any event that may negatively impact the FPKI Community and/or RPs, and therefore requires immediate attention and resolution (i.e., incident management).

A comprehensive IMP is essential because of the potential harm the FPKI Community and RPs may encounter from such events, and because of the scope, extent, and complexity of the extended FPKI Community and communication channels. See Appendix A for a case study that supports this need.

1.3 Audience

This is a public document intended for the entire FPKI community, RPs, and anyone else who may be interested.

1.4 Scope

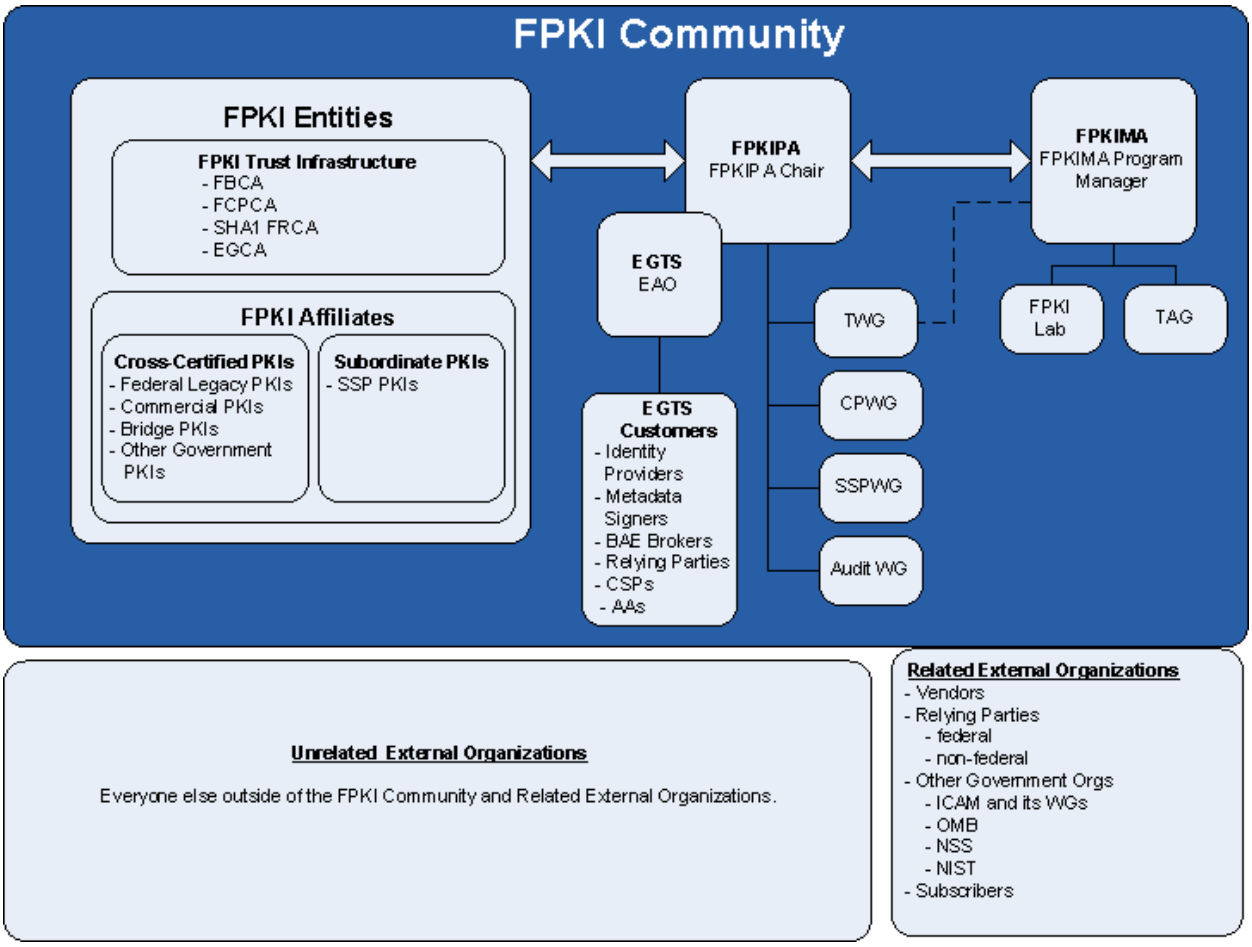
The scope of this document is limited to incident management. This includes, but is not limited to roles and responsibilities, and the categorization and prioritization of incidents, and response communication and coordination.

Problem management (i.e., root cause analysis with the goal to prevent the incident from reoccurring) is out of scope.

2 Description of the FPKI Community

The FPKI Community is comprised of government and commercial organizations, which enable trust for interoperable, high-assurance person, entity, or NPE identity authentication. For a complete description of the FPKI Community, see *Federal Public Key Infrastructure (FPKI) Concept of Operations (ConOps)* [FPKI ConOps]. Figure 2 summarizes the organizational composition of the FPKI.

Figure 2. High-level FPKI Organization



2.1 The FPKI Policy Authority (FPKIPA)

The FPKIPA is the FPKI governing body that develops digital-certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies. FPKIPA working groups include:

- FPKI Technical Working Group (FPKI TWG)
- Certificate Policy Working Group (CPWG)
- Shared Service Provider Working Group (SSPWG)
- Audit Working Group (Audit WG)

2.2 The FPKI Management Authority (FPKIMA)

The FPKIMA operates, maintains, and manages the FPKI Trust Infrastructure on a day-to-day basis in accordance with the Federal X.509 Certificate Policies and the Certification Practice Statements approved by the FPKIPA. In addition, the FPKIMA maintains and operates an FPKI Lab, facilitates the TWG on behalf of the FPKIPA, and includes the Technical Advisory Group (TAG).

2.3 FPKI Entities

There are five categories of FPKI Entities in connection with the FPKI Trust Infrastructure:

- Legacy PKIs
- Bridge PKIs
- SSP PKIs
- Commercial PKIs
- Other government PKIs

2.4 Related External Organizations

To execute its mission, the FPKI interfaces with, and depends upon various external organizations with whom there is no direct relationship. These organizations include:

- Relying Parties
- Vendors
- Other Government Organizations
- Subscribers

2.5 Unrelated External Organizations

Unrelated organizations are those that are neither in the FPKI Community nor a related FPKI external organization. Though unrelated external organizations have no ostensible relationship with or interest in the FPKI, the FPKI may ultimately be affected, directly or indirectly, by actions (malicious or otherwise) of those organizations. An example of an unrelated external organization is DigiNotar (see Appendix A-1).

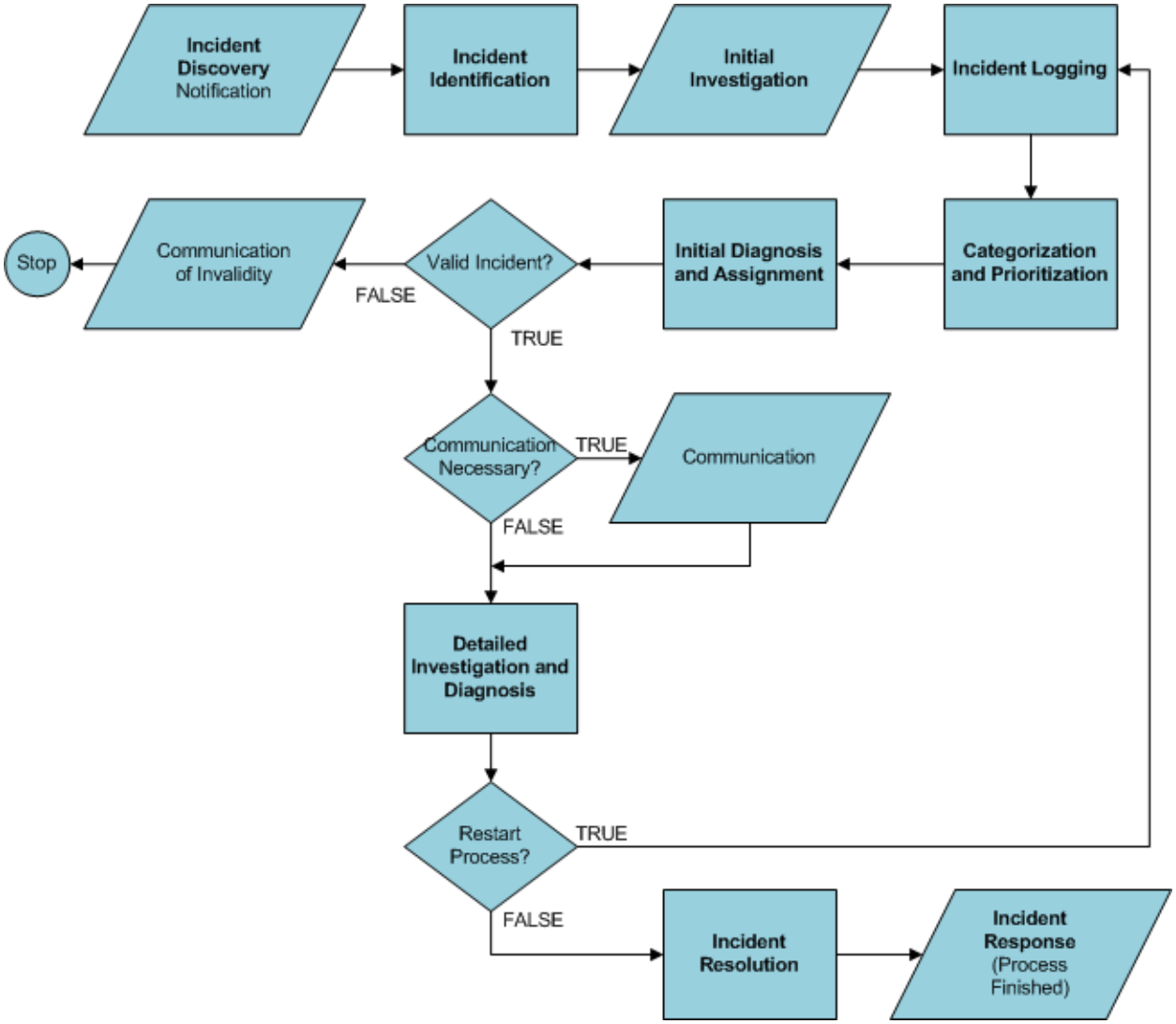
3 The Incident Management Process

The FPKI Community Incident Management Process is maintained by the FPKIPA (the Process Owner), and administered by the FPKIMA (the Process Manager). The FPKIPA is responsible for approving this process, as documented herein, and the outcome of incidents handled by this process (or non-incidents dismissed by this process). The FPKIMA manages execution of this process, which consists of six phases:

1. Incident Discovery and Identification;
2. Initial Investigation and Incident Logging;
3. Categorization and Prioritization;
4. Initial Diagnosis and Assignment;
5. Detailed Investigation and Diagnosis; and
6. Incident Response Resolution.

These phases are detailed in the following six sub-sections. Throughout the phases, all IMP participants communicate, coordinate, and collaborate with each other as necessary. Figure 3 illustrates the flow of the entire IMP.

Figure 3 The FPKI Incident Management Process



3.1 Phase 1: Incident Discovery and Identification

At the direction of the FPKIPA, the FPKIMA has been delegated the responsibility of identifying FPKI Community incidents, and initiating the IMP if appropriate. It is extremely important for the FPKIMA, FPKIPA, and all other FPKI Community members to monitor all incident-notification sources closely. If an incident goes undetected, it cannot be identified and processed, which in most cases increases the severity of potential impacts. Incident sources are infinite and always evolving. Some of the key incident-notification sources include:

- Department of Homeland Security (DHS)
  - United States Computer Emergency Readiness Team (US-CERT)

        - http://www.us-cert.gov/cas/signup.html
    - Federal Emergency Management Agency (FEMA)
        - Integrated Public Alert and Warning System (IPAWS)
        - Emergency Alert System (EAS)
- National Security Agency (NSA) / Central Security Service (CSS)
    - Information Assurance Service Center
- National Institute of Standards and Technology (NIST)
    - Information Technology Laboratory (ITL), Computer Security Division (CSD)
    - Computer Security Resource Center (CSRC)
- Internet Storm Center (ISC)
- Certification Authority Browser (CAB) Forum
- Other federal agencies responsible for security, audit, or interagency communications
- An FPKI Community member
    - Reporting on observations while monitoring the production environment (internal or external to the FPKI Community member's organization)
    - Reporting on knowledge obtained (internal or external to the FPKI Community member's organization)
- Direct notification from a vendor
- Public news providers, public forums, blogs, email distributions, and so on.

An incident can only be subject to this IMP if it is discovered by the FPKIMA, or the FPKIMA is notified of the discovery. The FPKIMA must be notified as early as possible of any FPKI-relevant incidents discovered by any FPKI Community member. The FPKIMA can be notified directly, or via the FPKIPA (if whoever is submitting the notification is obligated to contact the FPKIPA, or the submitter is the FPKIPA). However, the FPKIMA does not limit the acceptance of incident discovery notifications to the FPKI Community. The earlier an incident is identified and addressed by this process, the earlier it can be mitigated. Contact information for the FPKIMA can be found on the IDManagement.Gov website. The Incident Discovery Notification Report in Appendix B may be used to facilitate the notification process. However, this Incident Discovery Notification Report is not a requirement.

3.2 Phase 2: Initial Investigation and Incident Logging

The FPKIMA must record all identified incidents, and perform the initial investigation for gathering details. The incident details are logged in an incident database maintained by the FPKIMA. The incident database is used to track incidents from identification through resolution, and is a data source for knowledge management in support of future incident management investigations. In turn, the initial investigation should include a review of past incident log records for similar incidents and supporting information.

During the initial investigation and incident logging, all identified incidents are logged with no validation checking or discrimination involved. The incident log captures:

- The name/title of the incident;

- The date and time of the incident identification;
- The date and time the incident/event began;
- The incident notification source; and
- A detailed description of the incident, as understood during this preliminary phase.

In addition, each incident is categorized and prioritized as detailed in the next section.

3.3 Phase 3: Categorization and Prioritization

The FPKIMA adds category information and priority information to the incident database log record. The incident is categorized and prioritized so that personnel and any automated support systems can handle it appropriately.

3.3.1 Categorization

All reported incidents are categorized using three sets of data relating to the incident: Incident Type, Incident Location, and whether or not the incident involves the compromise of a CA (CA Compromise).

3.3.1.1 Incident Type

There are eight optional Incident Types. The Incident Type category enables the FPKIMA to classify each incident, and to assist in detailing and understanding the description of the incident. Table 1 lists the Incident Type categories.

Table 1 FPKI Incident Types

Incident Type
Malicious Attack
Risk (Security)
Risk (Legal)
Risk (Financial)
Risk (Other)
Hardware/Software Error
Manual Error
Environmental Disaster

1. **Malicious Attack**: A forceful act by one entity, with potential negative impacts on another entity (or entities), such as a system being compromised by a “hacker” (e.g., viruses, worms, denial of service), or a bomb being detonated at a target facility.
2. **Risk (Security):** An event or condition that creates or suggests the potential of a security breach, such as the identification of an application or hardware device vulnerability.

3. **Risk (Legal):** An event or condition that creates or suggests the potential of negative impacts associated with a legal liability, such as a lawsuit in which the claim challenges the validity of a service provided by a system.
4. **Risk (Financial):** An event or condition that creates or suggests the potential of negative impacts associated with financial imbalance, such as a major decrease in budget.
5. **Risk (Other):** An event or condition that creates or suggests a negative impact that's not covered by one of the three vulnerabilities detailed above.
6. **Hardware/Software Error:** An unanticipated failure of hardware or software, such as a program "bug" causing the generation of erroneous system data.
7. **Manual Error:** Negative impacts to a system caused by improper execution of procedures, such as an accidental deletion of vital system data.
8. **Environmental Disaster:** An unanticipated disaster causing negative impacts to a system, such as hurricane, earthquake, fire, air conditioner failure, or sprinkler system malfunction.

3.3.1.2 Incident Location

The incident location is where the incident appears to occur, as reported by the discovery source or as determined during the initial investigation. This does not necessarily mean that the location will prove to be the origin of the incident. The origin of an incident is confirmed during the Initial Diagnosis and Assignment phase or the Detailed Investigation and Diagnosis phase, and the incident location is a significant input and resource to those phases.

Incidents may occur at the FPKI Trust Infrastructure, an Affiliate PKI, a related external organization, or an unrelated external organization. Table 2 depicts the incident location category and its optional selections. If more location detail can be provided (e.g., a specific Affiliate, a specific system, a specific component, a specific capability), then that should be included in the incident description field of the log record.

Table 2 Examples of FPKI Incident Locations

FPKI Incident Location
FPKI Affiliate: FCPCA Cross-Certified PKI
FPKI Affiliate: FCPCA Subordinate PKI
FPKI Affiliate: FBCA Cross-Certified PKI
Related External Organization
Unrelated External Organization
FPKI Trust Infrastructure: FCPCA
FPKI Trust Infrastructure: FBCA
FPKI Trust Infrastructure: SHA1 FRCA
FPKI Trust Infrastructure: EGCA
FPKI Trust Infrastructure: Repository

Examples:

1. If the FBCA crashes and the FPKIMA is unable to restore the service before its Certificate Revocation List (CRLs) expire, the incident location is “Trust Infrastructure: FBCA.”
2. If Microsoft announces a high-risk vulnerability related to the Cryptographic Application Programming Interface (CAPI), which is commonly relied on for certificate management in the FPKI environment, the incident location is “Related External Organization.”
3. When the DigiNotar CA was compromised, the incident location was “Unrelated External Organization.”

3.3.1.3 CA Compromise

There are two optional CA Compromise selections: True or False. CA compromises are of particular interest to the FPKI Community, as trust relationships may be established directly or indirectly with the compromised CA. The category is relevant to any CA, whether a member of the FPKI or not, as many CAs external to the FPKI community are distributed by application vendors as trusted CAs. A CA compromise means that the CA system was successfully accessed in a manner that is not authorized, thus putting access to the CA’s private key at risk of unauthorized access, diminishing the integrity of the data on the CA system, and reducing the level of trust in certificates issued by that CA.

The CA Compromise selection is a key factor for trending and analysis, and is significant input for the prioritization selections and the Initial Diagnosis and Assignment phase. Table 3 lists the CA Compromise categories.

Table 3 CA Compromise

CA Compromise
True
False

If the CA Compromise is “True,” the description in the log record must clearly identify the compromised CA.

3.3.2 Prioritization

The priority of an incident is used to identify the relative importance of an incident. Prioritization is an important consideration because it determines how personnel and support tools process the incident. Priority is based on the urgency, scope of the FPKI Community affected, and the impact severity of the incident. As detailed in Table 4, FPKI community incidents are prioritized based on urgency, the potential community scope, and four potential impact severity factors.

Table 4 Incident Prioritization Matrix

Prioritization Factor 1	Prioritization Factor 2	Prioritization Factor 3			
Urgency	Potential Community Scope	Potential Security Impact Severity	Potential Operational Impact Severity	Potential Legal Impact Severity	Potential Financial Impact Severity
(3) High	(3) High	(3) High	(3) High	(3) High	(3) High
(2) Medium	(2) Medium	(2) Medium	(2) Medium	(2) Medium	(2) Medium
(1) Low	(1) Low	(1) Low	(1) Low	(1) Low	(1) Low
(0) None	(0) None	(0) None	(0) None	(0) None	(0) None

The numeric value of the overall priority level is determined by taking the average of the urgency (factor 1) , potential scope of the FPKI Community affected (factor 2), and highest value from the potential impact severities (factor 3). The algorithm is summarized below:

Priority = ((factor 1 + factor 2 + highest value in factor 3) / 3)

The descriptive label of the overall priority level is based on the numeric value using Table 5:

Table 5 Overall Priority Label

Overall Priority Label	
2.5 < numeric value	High
2 < numeric value ≤ 2.5	Medium/High
1.5 < numeric value ≤ 2	Medium
1 < numeric value ≤1.5	Low/Medium
numeric value ≤ 1	Low

For example, if an incident is given the priority selections specified in Table 6, the overall priority has a numeric value of 2.33, as a result of (2+2+3)/3 . The overall priority is labeled as Medium/High, and the 2.33 value can be used if an incident-triage decision is required (i.e., address the incident with the highest numeric value first).

Table 6 Example Prioritization

Prioritization Factor 1	Prioritization Factor 2	Prioritization Factor 3			
Urgency	Potential Community Scope	Potential Security Impact Severity	Potential Operational Impact Severity	Potential Legal Impact Severity	Potential Financial Impact Severity
(2) Medium	**(2) Medium**	(2) Medium	**(3) High**	(0) None	(1) Low

It is important that values be assigned objectively (i.e. solely in accordance with analysis findings). A tendency towards a particular value (e.g., always assign High) may undermine the entire prioritization step.

Details of each factor in the above example are discussed in the following sub-sections.

3.3.2.1 Urgency

Urgency is strictly a measure of how long it will take before the incident has the potential of significantly impacting the FPKI Community. Urgency does not take the severity of the impact into account. Use Table 7 as a guide in determining the urgency level.

Table 7 Urgency Levels

Urgency	
Significant Impact is estimated to occur in:	**Severity Level**
15 calendar days or less	High
15 – 90 calendar days	Medium
More than 90 calendar days	Low/None
Unknown	Unknown

3.3.2.2 Potential Community Scope

The Potential Community Scope is used to identify all areas of the FPKI Community that may be impacted by the incident. This factor does not take the impact severity on the community into account, but rather concentrates on who may be impacted. Table 8 includes community scope criteria for each selection level.

Table 8 Levels of Potential Community Scope

Potential Community Scope	
Criteria	**Level**
Entire FPKI Community	High
FPKI Subscribers and/or RPs from multiple FPKI Entities	Medium
Limited to a single FPKI Entity's Subscribers and/or RPs	Low/None
Unknown	Unknown

3.3.2.3 Impact Severity Factors

Determinations for the four potential impact severity factors are dependent on expert analysis and judgment. In analyzing the potential impact severities, all of the potential direct and indirect results of the incident must be considered, including the possibility that there will be additional instances of the incident. The potential impact criteria detailed in

Table 9 contain some relative terms, like “significant,” “severe,” “serious,” “major,” and “minor,” whose meaning will depend on context. The FPKIMA must consider the context and the nature of the incident impacts, and their probability, to decide the relative significance. Table 9 includes criteria for each level, in support of the four impact severity factors.

Table 9 Potential Impact Severity Levels

Potential Impact Severity Levels	
Criteria	**Level**
The incident has significant potential of a catastrophic effect on the FPKI community’s security posture, operations, legal standing, or financial standing. A catastrophic effect means that, for example, the incident might: (1) present plausible threats to invalidate the FPKI’s confidentiality, integrity, non-repudiation, or authentication services; (2) result in loss of life or serious life threatening injuries; (3) cause a severe degradation in or loss of mission capability to an extent and duration that the FPKI is not able to perform one or more of its primary functions; (4) result in major legal liability; or (5) result in major financial loss.	High
The incident could have a serious adverse effect on the FPKI Community’s security posture, operations, legal standing, or financial standing. A serious adverse effect means that, for example, the incident might: (1) present significant threats to the level of confidentiality, integrity, non-repudiation, or authentication services provided by the FPKI; (2) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries; (3) cause a significant degradation in mission capability to an extent and duration that the FPKI is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (4) result in significant legal liability; or (5) result in significant financial loss.	Medium
The incident could have a limited adverse effect on the FPKI Community’s security posture, operations, legal standing, or financial standing. A limited adverse effect means that, for example, the incident might: (1) present minor threats to the level of confidentiality, integrity, non-repudiation, or authentication services provided by the FPKI; (2) cause a degradation in mission capability to an extent and duration that the FPKI is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (3) result in minor legal liability; or (4) result in minor financial loss.	Low
The incident has no potential for adverse effects in the associated area.	None

3.4 Phase 4: Initial Diagnosis and Assignment

The FPKIMA performs the initial diagnosis and assignment, starting with the information gathered and entered into the log record thus far. This is often done by the same individual(s) who logged, categorized, and prioritized the incident, and is often treated as one activity. The goal of the initial diagnosis and assignment is to determine precisely what has gone wrong (if anything) so, in turn, necessary parties can be notified and the path to resolution can be established. Specifically, the FPKIMA will seek to make three determinations, in producing the output of this phase:

1. Is this a valid incident or is it a false alarm?
2. FPKI community communication: Is one required? What details are necessary? Who needs to be included?
3. Incident assignment and recommendations (for valid incidents only): Assign an incident Response Lead, and provide them with high-level resolution recommendations based on the initial diagnosis.

As the initial diagnosis and assignment completes, the above determinations are detailed in the incident log record, and provided for the next phase.

3.4.1 Determination of Incident Validity

When the FPKIMA determines that the reported incident is actually a false alarm, a communication is sent to any relevant parties. This will often include the FPKIPA Chair and entity that reported the incident. If the incident claim has received much exposure, it may be necessary to communicate the incident invalidity to the entire FPKI Community. In any case, the process is stopped prior to expending further resources on a detailed investigation and diagnosis and incident response resolution. The log record is updated with the information supporting the decision to identify it as a false alarm, and closed, but the record remains in the incident database for trending and analysis.

3.4.2 Immediate/Initial Communication

The FPKIMA must decide whether an incident requires an immediate communication with individuals or organizations outside of the FPKIMA before the detailed investigation and diagnosis, and if so, who to include in the communication. The following rules should be used in making that determination:

- All members of the FPKIMA, including the Program Manager, are informed of all incident discovery notifications.
  - FPKIPA-MA@LISTSERV.GSA.GOV
- In addition to the above, all incidents that are determined to be valid within the initial diagnosis and investigation require immediate communication to the FPKIPA.
  - FPKIPA@listserv.gsa.gov
- In addition to the above, all valid CA compromise incidents require immediate communication to the FPKIPA customers, FPKI Certificate Policy Working Group (CPWG), and the FPKI technical Trust Infrastructure practitioners (TTIPS).
  - FPKIPA_CUSTOMERS@LISTSERV.GSA.GOV
  - FPKIPA_CPWG@LISTSERV.GSA.GOV

- FPKI-TTIPS@LISTSERV.GSA.GOV
- All incidents with a medium or high impact severity also require an immediate communication to the FPKIPA Community, FPKI CPWG, and Entity technical representatives.

These are the baseline rules. The FPKIMA is responsible for evaluating each incident individually and making the determination when further communication requirements are appropriate. Depending on the nature of the specific incident, there may be times when it's appropriate to attempt to notify as many RPs as possible. It may be necessary to leverage the Identity, Credential and Access Management Subcommittee (ICAMSC) for communications to the relying parties within the wider Federal Community. It may be necessary to notify US-CERT, FEMA, NSA, NIST, ISC, CAB Forum, or other organizations, and leverage their ability to reach RPs internal and external to the FPKI.

3.4.3 Incident Assignment and Recommendations

The FPKIMA must assign the incident to the appropriate organization, as the Response Lead. If the incident is directly related to an FPKI Entity, the incident will be assigned to that member. In many cases though, the incident will stay assigned with the FPKIMA, as the FPKIMA is responsible for the centralized FPKI Trust Infrastructure components. Further, the FPKIMA will be assigned external incidents, responsible for providing any guidance and/or communications deemed necessary. In all cases, the FPKIMA will stay engaged with the incident management process in a coordination role, keep the log record up to date, and take responsibility for community-wide communications on behalf of the FPKIPA.

The incident location specified in the log record will often provide the information needed to determine the appropriate Response Lead. However, the identification of a specific organization often requires the analysis of further details. The FPKIMA will thoroughly review all other details of the incident, and perform any preliminary research needed to determine the appropriate incident assignment. Along with the incident assignment, the FPKIMA will also establish and provide high-level resolution recommendations as part of the initial diagnosis and assignment responsibilities. The assignment and the resolution recommendations will be added to the log record.

A timeline is included in the recommended resolution, based on the incident's urgency level. All incidents will include a resolution and response due date, within the timeframe detailed in the corresponding urgency level (e.g., high urgency incidents will have a resolution and response due date within 15 calendar days of the incident identification). However, the FPKIMA is responsible for evaluating each incident individually and making the determination when more stringent due dates are appropriate. A higher-impact severity level and/or community scope may influence the timeline to be tighter than what the urgency level demands.

3.5 Phase 5: Detailed Investigation and Diagnosis

A valid incident shall proceed to the Detailed Investigation and Diagnosis phase. Throughout the Detailed Investigation and Diagnosis phase, the FPKIPA shall stay engaged, either as a contact to an external Response Lead or as a consulting body to the FPKIMA. Additionally, the FPKIPA shall be responsible for communications with the FPKI Community regarding the incident. However, the FPKIPA may delegate communication responsibilities to others (e.g., the FPKIMA).

The purpose of the Detailed Investigation and Diagnosis phase is to determine the origin of the incident (i.e., the triggering event), determine the extent of any current or potential impacts on the FPKI Community, and develop a remediation recommendation to stop this incident from resulting in any future negative impacts. Depending on the origin of the incident, this plan may involve the FPKIMA taking direct, corrective action or the FPKIPA providing guidance and recommendations out to the FPKI Community.

Inputs into the Investigation and Diagnosis phase include:

- The incident log record;
- Incident assignment, including contact information for the FPKIMA, FPKIPA, Response Lead, and any organization assigned to a support role; and
- High-level resolution recommendation, including suggested timeline.

Investigation and diagnosis of an incident may include the following activities:

- Identifying the origin of the incident;
- Establishing exactly what has gone wrong;
- Understanding the chronological order of events;
- Confirming the full impact of the incident;
- Identifying any events that could have triggered the incident;
- Searching knowledgebase for any previous incidents, problems, or known errors that may be involved in the incident; or
- Identifying an appropriate resolution.

3.5.1 Incident Investigation

Incident Investigation attempts to identify the origin of the incident (i.e., trigger event or events that caused the incident). Incident investigation assumes the FPKI would have properly operated indefinitely had a triggering event not occurred and that all external dependencies (i.e., network infrastructure, third-party products, and service providers) are accounted for.

If it has not been done so already, an analysis shall be performed as to what may have triggered the incident. Possible triggers include:

- A change to a PKI or other system (either internal or external to the FPKI Community) that has unintended consequences on an FPKI Community Affiliate, FPKI subscribers, or FPKI RPs;
- Malicious activity targeting either the FPKI Trust Infrastructure or another FPKI Community entity;
- Malicious activity targeting an external entity, which may negatively impact an FPKI Community Affiliate, FPKI subscribers, or FPKI RPs; and
- A policy or procedure violation, which may negatively impact an FPKI Community Affiliate, FPKI subscribers, or FPKI RPs.

If the Response Lead is the FPKIMA, an analysis of the incident's triggering events and factors may be performed by the FPKI Technical Working Group (TWG) in consultation with the FPKIPA, the CPWG, and any applicable external entities.

3.5.2 Impact Assessment

Regardless of the incident's origin, an assessment shall be performed to determine the extent of any current or potential impacts on the FPKI Community. This assessment shall be performed by the FPKIMA in consultation with the FPKI TWG or CPWG if necessary. Inputs to this process may include:

- System architecture diagrams;
- FPKI CA cross-certificates;
- SSP agreements;
- Memorandums of Agreement (MOAs);
- Points of contact list for FPKI Entities;
- Certificate Policies; and
- Publicly-available information describing the incident.

3.5.3 Remediation Recommendation

A remediation recommendation is established to stop the incident from resulting in any future negative impacts on the FPKI community. Depending on the triggering event and impact assessment, immediate action may be warranted to eliminate the incident and restore the service to proper operating status. Examples of possible remediation actions include:

1. Rolling back the appropriate system(s) to the state prior to triggering the incident;
2. Revoking the cross-certificate issued to the affected CA;
3. Removing the affected CA's certificates from applicable trust stores;
4. Installation of a software patch or hot fix; or
5. The development and issuance of applicable guidance to FPKI Entities.

If the FPKIMA is the Response Lead, a recommendation for remediation actions will be developed in consultation with the FPKI CPWG and/or FPKI TWG as necessary, and provided to the FPKIPA for approval. The recommendation may take the form of an emergency system change request or, if available, activation of a roll-back plan. The remediation recommendation should also include a timeframe for implementation.

The FPKIPA shall make the decision whether or not to implement the remediation action based on the remediation recommendation provided by the FPKIMA. Alternatively, the FPKIPA may request additional information from or a consultation with the CPWG or FPKI TWG.

In cases where the assigned Response Lead is external to the FPKIMA, the FPKIPA may request that remediation guidance be published for the FPKI Community to view. The FPKIPA may delegate the writing and distribution of remediation guidance to the FPKIMA, CPWG, or TWG as appropriate.

Table 10 provides some examples of triggering events with the remediation action that may be recommended:

Table 10 Triggering Events and Recommended Remediations

Triggering Event	Recommended Remediation
Compromise of a CA with a direct trust relationship to the FPKI Trust Infrastructure.	Will likely be for revocation of the associated cross-certificate(s), and dissemination of guidance to the FPKI Community to ensure that the compromised CA's certificate has been removed from trusted root stores and repositories.
Compromise of a CA external to the FPKI (i.e., not cross-certified with the FPKI Trust Infrastructure).	Will likely require FPKI Community guidance dissemination to ensure that the compromised CA's certificate has been removed from trusted root stores and repositories.
Violations of a CA's Certificate Practice Statement, or other procedural violations, that do not result in a known compromise of that CA.	May or may not include revocation of the affected CA's cross-certificate(s). In addition, the FPKI may issue guidance to the FPKI Community notifying them of the violation and advising them of the risks associated with continuing to trust the affected CA.
Identification of a software bug or vulnerability causing path discovery or validation errors.	Will likely require the vendor to implement a patch or hot fix. The FPKIMA will work with the vendor and the FPKI Community to disseminate guidance detailing the cause and effect of the error, and the patch or hot fix to correct it.

In any case, a recommended remediation plan is developed by the Response Lead with support from the FPKIMA (if the FPKIMA is not the Response Lead), and the TWG and/or CPWG if necessary. The plan is presented to the FPKIPA Chair for approval. The remediation plan will detail the required remediation actions and an implementation timeline.

Based on the incident investigation and impact assessment, the FPKIPA Chair will determine if the remediation plan requires approval from other FPKIPA members, and/or communication to other members of the FPKI Community. However, any remediation plan associated with incidents given a [medium or high potential community scope] and a [medium or high impact severity] require communication to the voting members of the FPKIPA, giving the members a chance to express any concerns with the plan. Depending on the feedback from the FPKIPA members and the incident urgency, the FPKIPA Chair may choose to hold an FPKIPA vote on the approval of the remediation plan.

3.5.4 Incident Remediation Logging

All validated incident origins, triggers, and remediation recommendations shall be input into the incident log record. The log will be updated with the new information discovered during the Detailed Investigation and Diagnosis phase. A decision will be made as to whether the log data is complete and accurate enough for use in the Incident Response Resolution phase, or the IMP needs to return to an earlier phase (see Figure 3).

3.6 Phase 6: Incident Response Resolution

The FPKIMA and the Response Lead (if the Response Lead is not the FPKIMA) is responsible for the Incident Response Resolution via execution of the approved remediation plan.

3.6.1 Remediation Action

As appropriate, any action(s) recommended and approved as part of a remediation plan in the Detailed Investigation and Diagnosis phase shall be implemented in accordance with applicable documented policies, practices, and procedures. Any effects of these actions shall be analyzed and a determination made as to whether the remediation has resolved the incident, or if further action is required. The FPKIPA will track the progression and status of the remediation action(s) and ensure adherence to the implementation timeline. If a remediation action is not implemented within the designated timeline, the FPKIPA may choose to reassess the incident and approve the invocation of an alternate remediation plan. For example, if a CA vulnerability is not mitigated within the designated timeline, the FPKIPA may choose to revoke a cross-certificate issued to that CA.

3.6.2 Communication

The purpose of this activity is to communicate incident status, including details of the resolution and any applicable guidance to all relevant parties. The FPKIPA is responsible for determining what information should be communicated, to whom, and by what means. At a minimum, all recipients (if any) of an initial communication during the Initial Diagnosis and Assignment Phase must receive the Incident Response Resolution communication as a follow-up. It may be determined however, that a wider audience should be included in this communication. In some cases the communication is the remediation action.

3.6.3 Reporting

The intent of the Reporting activity is to capture any information learned from the incident for the future reference of the FPKIPA, the FPKIMA, and if appropriate, others in the FPKI Community. Such data should be considered when future changes are assessed or during the design phase for any system upgrades.

All pertinent actions and effects shall be captured in the incident database. Additionally, if applicable, the incident's triggering event(s), impact, and resolution shall be entered into any other knowledgebase or similar searchable, lessons learned database.

3.6.4 Long-term Actions

Prior to closing out the incident, the following actions shall be considered:

- If a system defect was identified as the source of or contributor to an incident, a change request shall be initiated to correct the defect.
- Any updates to the operating policies shall be initiated through the appropriate process.
- If applicable, an after-action report shall be completed and submitted to the appropriate authoritative body.
- Contingency actions identified during the Incident Investigation phase shall be implemented.

- If a previously unknown effect was discovered or new best practice developed, a whitepaper or other industry-wide communication may be published under the auspices of the FPKIPA.

4 Roles and Responsibilities

The actual Roles that will be called on for approval and consultation may vary depending on the type and priority of the incident. Regardless of the incident type, all FPKI Community members shall be informed of an incident and the FPKIMA will take responsibility for collaborating with the other roles to reach a recommendation on appropriate actions to be taken. The FPKIPA will provide the ultimate approval of the final Incident Response Resolution.

In addition, it is the responsibility of each FPKI Entity to disseminate the information to their users and customers, as appropriate. Table 11 summarizes the responsibilities for each IMP role. The responsibilities are as follows:

- **Recommend/Responsible (R)** – ensure the necessary activities of a given phase are completed, or manage the inputs from various sources to develop the required output of that phase. In most phases this includes developing a recommendation.
- **Approve (A)** – gives final approval of any incident response resolution decision.
- **Consult (C) –** consulted or provides input before an activity is performed or a decision is taken.
- **Informed (I)** – Those who need to be informed after (or during) an activity is performed or a decision is taken.

Table 11 Incident Handling Responsibilities by Role

FPKI Community Member	Incident Discovery and Identification	Initial Investigation and Logging	Categorization and Prioritization	Initial Diagnosis and Assignment	Detailed Investigation and Diagnosis	Incident Response Resolution	Communications
FPKIMA	R	R	R	R	R	R	R
FPKIPA	A/R	A/I	A/I	A/I/C	A/I/C	A	A/R
Affiliates	R	I	I	I/C	I/C	I/C	R
CPWG	R	I	I	I/C	I/C	I/C	I
TWG	R	I	I	I/C	I/C	I/C	I
Vendors	R	I	I	I/C	I/C	I/C	I
Federal RPs	R	I	I	I/C	I/C	I/C	I

4.1 Federal PKI Policy Authority (FPKIPA)

The FPKIPA is the Process Owner for the FPKI Community IMP. The FPKIPA and the FPKIPA Chair must consider technical, policy, and business impacts when responding to incidents.

While the FPKIPA Chair has authority to take action in emergency situations (e.g., an emergency revocation due to a CA compromise), the FPKIPA, as the governing body for the FPKI, will approve longer-term actions in response to incidents. FPKIPA responsibilities in terms of incident management include:

1. Approving Incident Response Plans and tactics (e.g., the FPKIPA may approve preset Standard Operating Procedures to handle specific types of incidents);
2. Approving response plans for specific incidents including:
    a. Directs Working Groups to perform analyses of various issues related to existing or potential future incidents.
    b. Approving Certificate Policy changes as a result of recommendations and analysis of incidents by FPKI working groups to enhance requirements and prevent or reduce future incidents.
    c. Publishing guidance related to or resulting from incidents.
    d. Approving operational changes in support of policy or in response to incidents.
    e. Authorizing (in non-emergency situations) the revocation of a cross-certificates to Entity CAs in the event revocation is recommended after analysis by FPKI Working Groups.
3. Communications including:
    a. Providing notification to the FPKI Community of specific incidents.
    b. Providing information on the planned response, its status, and long term plans for resolution.
    c. Coordinating development and distribution of lessons learned updates.
    d. Public Relations and press releases about specific incidents.
4. Intra-FPKI coordination and communication, and coordination with other government organizations including:
    a. Coordination with NIST, OMB or other Government organizations.
    b. Coordination and Communication with FPKI Affiliates impacted by specific incidents.
5. Coordinating and Communicating with External Organizations including:
    a. Coordination with Vendors and RPs.
6. Coordinating with FPKI Legal Counsel as needed.

4.1.1 FPKIPA Working Groups

4.1.1.1 FPKI Technical Working Group (TWG)

The FPKIMA and FPKIPA may call upon the FPKI TWG to support Detailed Investigation and Diagnosis or Incident Resolution.

After an incident is resolved, the associated Problem Management task to identify the cause of the incident and prevent it from happening again may be assigned to the FPKI TWG. This may include

developing a white paper, research, developing tests, or coordinating with vendors or other FPKI Community members.

4.1.1.2 Certificate Policy Working Group (CPWG)

During incident management, the CPWG is mainly an observer (i.e., interested party). However, the CPWG has an active role once incident management has transitioned into problem management. The CPWG may analyze impacts of incidents and evaluate methods for enhancing policy to avoid similar incidents in the future. In addition, the CPWG will receive technical analyses of specific incidents or threats from the FPKI TWG or other sources and work to develop policy supporting technical solutions that counter the threats and reduce the risk of occurrence for particular incidents. As a result of the CPWG policy analysis, the CPWG will recommend policy changes to the FPKIPA to address weaknesses in policy exposed by incidents.

4.2 Federal PKI Management Authority (FPKIMA)

Along with all members of the FPKI Community, the FPKIMA observes incident sources and stays ready for incident discovery. The FPKIMA is responsible for accepting incident reports from other members of the FPKI Community. The FPKIMA is responsible for:

- Incident Identification;
- Initial investigation and incident logging;
- Categorization and prioritization;
- Initial diagnosis and assignment;
- Detailed Investigation and Diagnosis; and
- Incident Response Resolution.

As the FPKIMA is the FPKI Community IMP manager, the FPKIMA is always responsible for playing a coordination and communication role in both Detailed Investigation and Diagnosis and Incident Response Resolution. However, the Response Lead may be assigned to another member of the FPKI Community, depending on the incident locations, origin of the incident, or results of the Initial Diagnosis.

The FPKIMA is responsible for coordinating with FPKI Entities, the FPKI TWG, the CPWG, or vendor when it is necessary for any of these other FPKI Community members to be involved with Detailed Investigation and Diagnosis or with Incident Resolution. As illustrated in

Table 11, when an FPKI Community member other than the FPKIMA is assigned Primary Lead for Detailed Investigation and Diagnosis and/or Incident Response, they are considered “consulting” as the ultimate responsibility for the process resides with the FPKIMA.

The FPKIMA is responsible for building a knowledge base of reported incidents to assist in developing responses for future incidents.

4.3 FPKI Affiliates

According to the FBCA and FCPCA certificate policies, as well as established MOAs, FPKI Affiliates are responsible for communicating any security incidents discovered regarding their own CAs to the FPKIPA.

If the FPKI Affiliate is required to report the incident to the FPKIPA, the FPKI Affiliate does not have to report the incident the FPKIMA, as the FPKIPA will convey the incident report to the FPKIMA.

Individual FPKI Affiliates may be called on to provide additional investigation and/or information about incidents directly affecting their PKI. Where Affiliates are also Bridges, the Affiliate will be the conduit for information between their members and the FPKI Community.

All FPKI Affiliates have the responsibility to communicate information about incidents to their own users and RPs.

FPKI Affiliates may be assigned as the Response Lead for the Detailed Investigation and Diagnosis phase and the Incident Response Resolution phase.

4.4 Relying Parties (RPs)

Any RP may initiate an incident report by sending information to the FPKIPA, who then notifies the FPKIMA. When an incident occurs that alters the trust in any part of the FPKI, information may need to be conveyed to RPs. Examples include, but are not limited to,

- A cross-certificate has been revoked and should be removed from any trust stores and direct trust configurations;
- A root certificate has been compromised;
- A patch is required to fix a potential security risk; and
- Certain configuration settings must be set to limit a security risk in a given application or operating system.

When information needs to be communicated to relying parties, the FPKIMA will coordinate with the FPKIPA, ICAMSC, and US-CERT, use the FPKI web site and other social media methods, and will rely on all FPKI Community members to disseminate the information to their own users.

4.5 Vendors

Any vendor may initiate an incident report by sending information directly to the FPKIMA or through any or all affected FPKI Affiliates. Depending on the details of an incident under investigation, a vendor may be requested to assist in the Investigation and Diagnosis phase.

If the incident is related to a compromise of a CA within the FPKI Trust Infrastructure or an FPKI Entity, the FPKIMA will provide information about the incident to vendors who distribute the FCPCA Root Certificate in their trust stores.

The FPKIMA will work to develop relationships with vendors and industry groups to improve communications between the FPKI Community and these external parties.

4.6 Identity, Credential and Access Management Subcommittee (ICAMSC)

The Federal Chief Information officers (CIO) Council established the Information Security and Identity Management Committee (ISIMC), charged with overseeing the government-wide activities related to Cybersecurity and Identity Management. The ICAM Subcommittee (ICAMSC) is one of four ISIMC

subcommittees, and is tasked with aligning the Identity Management activities of government, including the FPKIPA as one of six working groups under the ICAMSC umbrella.

As there are no limitations on who the FPKIMA accepts incident discovery notifications from, any member of the ICAMSC may report FPKI Community incidents. The relationship and similarities between the ICAMSC and the FPKI, makes the ICAMSC a likely candidate for discovering incidents that are relevant to the FPKI Community.

Depending on the type of incident and the recommended resolution, the ICAMSC may be assigned communication actions during the initial diagnosis and assignment or the incident response resolution. For example, since the FPKIPA cannot communicate directly with every federal RP, the FPKIPA may ask the ICAMSC to communicate with some or all federal RPs.

5 Tool Requirements

The FPKI Community IMP requires a mechanism for logging and tracking incidents in an incident database, and building a knowledge base for trending and analysis and supporting the investigation of new incidents. For that purpose, the FPKIMA will implement an Information Technology Service Management (ITSM) tool, Numara Footprints, during the 2012 calendar year. Numara will be used to log each incident (according to the specifications in Section 3) as a "ticket," and save it in the incident database. The tickets will be updated and tracked by the FPKIMA throughout the life of the incidents, and will be used to build the incident knowledge base.

Prior to the implementation of Numara, the FPKIMA will log, track, and store each incident in a customized Microsoft Access database.

The FPKIMA maintains various email distribution lists on behalf of the FPKI Community. These will be used for communication of incidents in support of this FPKI Community IMP:

- FPKIPA@listserv.gsa.gov - FPKIPA Member Representatives and FPKIPA observers. This list is used to distribute non-sensitive information amongst the FPKIPA community and interested parties, such as FPKIPA meeting announcements.
- FPKIPA_Officials@listserv.gsa.gov - FPKIPA Federal Member Representatives. This list is used to distribute information intended only for federal -employee representatives of the FPKIPA member organizations.
- FPKIPA_CPWG@listserv.gsa.gov - CPWG Participants. This list is used to distribute information to everyone that participates in the CPWG meetings.
- FPKIPA-MA@listserv.gsa.gov - FPKIMA Team Members. This list is used to distribute information to the FPKIMA.
- FPKIPA_Customers@listserv.gsa.gov - Technical Points of Contact (POCs) lists from the FPKI Community Members. This is a list of lists, as each FPKI organization provides the email lists for their technical POCs, such as helpdesk staff, to be included. This list is used to distribute information regarding operational status amongst the FPKI Community.

- FPKI-TTIPS@listserv.gsa.govlist - Technical Trust Infrastructure Practitioners – Technical Representatives from the FPKI Customer Organizations. This list is used as the FPKI TWG contact list.

A project is currently underway to make the IDManagement.gov website more interactive. This website will ultimately be a valuable tool for publishing, disseminating, and receiving communications. It will be utilized for incident discovery notifications and incident response communications.

Appendix A Case Studies

A-1 DigiNotar CA Compromise

On August 29, 2011, a public report revealed that a fraudulent google.com certificate had been issued by a DigiNotar CA and presented to a number of internet users in Iran. Immediate attention was required to determine any impacts on the FPKI Community and the appropriate response to such impacts. The below case study demonstrates how that incident would have fit into the phases of this IMP if it were in place at that time.

Phase 1: Incident Discovery and Identification

Discovery Source: The public Mozilla Security Blog (reported to Mozilla by Google, Inc.)

- http://blog.mozilla.com/security/2011/08/29/fraudulent-google-com-certificate/

Incident Identification: On August 30, 2011 the FPKIMA staff identified the August 29, 2011 report of a fraudulent Google.com certificate issued by the DigiNotar CA.

Phase 2: Initial Investigation and Incident Logging

Initial investigations by the FPKIMA uncovered the following supporting information:

- http://news.cnet.com/8301-27080_3-20098894-245/fraudulent-google-certificate-points-to-internet-attack/
- http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-man-in-middle.html
- http://technet.microsoft.com/en-us/security/advisory/2607712
- http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx

If the FPKI Community IMP were in place at the time, the incident log record would have contained the following:

- **Incident Name/Title** – DigiNotar CA Compromise
- **Date and Time of Incident Identification** – 8/30/2011 07:00am (ET)
- **Date and Time Incident Began** – 7/19/2011 ??:??
- **Notification Source** – Mozilla Security Blog, CNet.com, Google Online Security Blog, Microsoft Security Tech Center, Vasco.com
- **Incident Description** – A Fraudulent Google PKI certificate was issued by a DigiNotar Root Certification Authority (CA). DigiNotar is a commercial certificate provider from the Netherlands. The DigiNotar CA that issued the fraudulent certificate is a trusted CA by default in the PKI trust stores across various vendor applications. DigiNotar has revoked the certificate in question and is investigating the situation.

On July 19th 2011, DigiNotar detected an intrusion into its Certificate Authority (CA) infrastructure, which resulted in the fraudulent issuance of public key certificate requests for a number of domains, including Google.com. After detecting the intrusion, an external security audit concluded that all fraudulently issued certificates were revoked. Subsequently, it was discovered that at least one fraudulent certificate had not been revoked at the time. After being notified by Dutch government organization Govcert, DigiNotar took immediate action and revoked the fraudulent certificate.

The above links would also be included in the log record for supporting information.

Phase 3: Categorization and Prioritization

If the FPKI Community IMP were in place at the time, the following categorizations would have been added to the incident log record:

- **Incident Type** – Malicious Attack & Risk (Security)
- **Incident Location** – Unrelated External Entity
- **CA Compromise** – True

If the FPKI Community IMP were in place at the time, the following prioritizations would have been added to the incident log record:

- **Urgency** – (3) Medium
- **Potential Community Scope** – (4) High
- **Potential Security Impact Severity** – (3) Medium
- **Potential Operational Impact Severity** – (3) Medium
- **Potential legal Impact Severity** – (3) Medium
- **Potential Financial Impact Severity** – (3) Medium

The overall priority is (3.5) Medium/High

Phase 4: Initial Diagnosis and Assignment

Incident Validity: Yes. The various sources prove that this is in fact a valid Incident.

Immediate/Initial Communication: Yes. With coordination and approval from the FPKIPA Chair, the below email communication was sent on August 31, 2011 at 9:00am to FPKIPA-MA@listserv.gsa.gov, FPKIPA@listserv.gsa.gov, FPKIPA_Customers@listserv.gsa.gov, FPKIPA_CPWG@listserv.gsa.gov, and FPKI-TTIPS@LISTSERV.GSA.GOV.

All,

This message is being sent on behalf of Deb Gallagher.

We were recently made aware of a Fraudulent Google PKI certificate that was issued by DigiNotar Root Certification Authority (CA). DigiNotar has revoked the certificate in question and

is investigating the situation. See the following link for the press statement from VASCO, DigiNotar's parent company.

http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx

The DigiNotar Root CA in question issues SSL and EV SSL certificates and was distributed through most browser trust stores. The major browser vendors are taking action to remove or disable the DigiNotar CA from their trust stores.

Mozilla Notice - http://blog.mozilla.com/security/2011/08/29/fraudulent-google-com-cer

Google Notice - http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-man-in-middle.html

Microsoft Notice - http://www.microsoft.com/technet/security/advisory/2607712.mspx

Until the root cause of the issue and the extent of its impact are determined the DigiNotar Root CA should be considered UNTRUSTED. The recommended approach for mitigating the risk of UNTRUSTED CAs is to actively remove the Root CA certificate from the PKI trust stores across vendor products including Microsoft, Apple, Java, Adobe, Opera, and Mozilla. Mozilla has provided guidance on manually deleting the DigiNotar CA certificate from Firefox, http://support.mozilla.com/en-US/kb/deleting-diginotar-ca-cert.

The details for the DigiNotar Root CA are as follows:
Common Name (CN): DigiNotar Root CA
Serial Number: 0c 76 da 9c 91 0c 4e 2c 9e fe 15 d0 58 93 3c 4c
SHA1 Thumbprint: c0 60 ed 44 cb d8 81 bd 0e f8 6c 0b a2 87 dd cf 81 67 47 8c

Incident Assignment / Response Lead: FPKIMA

High Level Resolution Recommendation: FPKIMA to continue investigation. Within 15 days, provide a follow up communication and provide a plan for problem management, if necessary.

Phase 5: Detailed Investigation and Diagnosis

The FPKIMA discovers a September 5, 2011 interim report: *DigiNotar Certificate Authority Breach "Operation Black Tulip"* by Fox-IT. Fox-IT was given the task of investigating the DigiNotar breach and reporting the details of the findings. The report indicates that many DigiNotar CAs were hacked, and 531 fraudulent certificates were issued.

The FPKIMA discovers that an individual in Iran publicly claims to be responsible for the DigiNotar hacks on various forums.

The FPKIMA confirms that there are no cross-certified trust relationships between the FPKI and any of the DigiNotar CAs. Ensuring proper CA certificate trust store management will prevent any fraudulent certificates issued from the compromised DigiNotar CAs from having any impacts on the FPKI

Community. The FPKIMA identifies the need to develop PKI Trust Store Management guidance, via the FPKI TWG.

Phase 6: Incident Response Resolution

With coordination and approval from the FPKIPA Chair, the below email communication was sent on September 8, 2011 at 12:30pm to FPKIPA-MA@listserv.gsa.gov, FPKIPA@listserv.gsa.gov, FPKPA_Customers@listserv.gsa.gov, FPKPA_CPWG@listserv.gsa.gov, and FPKI-TTIPS@LISTSERV.GSA.GOV.

> *All,*
>
> *We are adding the topic of PKI Trust Store Management to the September 15 FPKI TWG meeting. The discussion will focus on the current practices in use to manage PKI Trust Stores and identify an approach for developing guidance to aid Federal Agencies in effectively managing PKI trust stores at the operational level. If any organizations have developed internal guidance on managing PKI trust stores please contact me as soon as possible, matthew.kotraba@pgs.protiviti.com.*
>
> *Additionally, attached is the public interim report from the independent third party investigation into the DigiNotar breach.*

In support of a long-term problem management effort, the development of an FPKI Trust Store Management Guidance document was initiated at the September 15 FPKI TWG, including the formation of an associated Tiger Team.

Appendix B Incident Discovery Notification Report

1) **Date and Time of Discovery:**
2) **Date and Time of Reporting:**
3) **Detailed Incident Description:**
4) **Discovery Source:** (*Identify your organization as the reporting organization, and identify any other sources that you relied on in gaining knowledge of the incident)*
5) **Incident Type:** *(Select all that apply)*
    - *Malicious Attack*
    - *Risk (Security)*
    - *Risk (Legal)*
    - *Risk (Financial)*
    - *Risk (Other)*
    - *Hardware/Software Error*
    - *Manual Error*
    - *Environmental Disaster*
6) **Incident Location:** *(Select all that apply)*
    - *FPKI Affiliate: FCPCA Cross-Certified PKI*
    - *FPKI Affiliate: FCPCA Subordinate PKI*
    - *FPKI Affiliate: FBCA Cross-Certified PKI*
    - *Related External Organization*
    - *Unrelated External Organization*
    - *FPKI Trust Infrastructure: FCPCA*
    - *FPKI Trust Infrastructure: FBCA*
    - *FPKI Trust Infrastructure: SHA1 FRCA*
    - *FPKI Trust Infrastructure: EGCA*
    - *FPKI Trust Infrastructure: Repository*
7) **CA Compromise:** *(Select one)*
    - *True*
    - False

Appendix C References

[FBCA CP] *X.509 Certificate Policy for the Federal Bridge Certificate Authority (FBCA)*
http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[FCPF CP] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*
http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf

[EGCA CP] *X.509 Certificate Policy for the E-Governance Certification Authorities*
http://www.idmanagement.gov/fpkipa/documents/EGovCA-CP.pdf

[FPKI ConOps] *Federal Public Key Infrastructure (FPKI) Concept of Operations (ConOps)*
http://www.idmanagement.gov/fpkipa/documents/FPKI Concept of Operations v1.0.0.pdf

Appendix D Glossary

Term	Definition
Analysis	The examination of acquired data for its significance and probative value to the case.
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
Availability	Timely and reliable access to and use of information.
Breach	An act from an outside organization that bypasses or contravenes security policies, practices, or procedures.
Community Risk	Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.
Compromise	A CA system was successfully accessed in a manner that is not authorized, thus putting access to the CA's private key at risk of unauthorized access, diminishing the integrity of the data on the CA system, and reducing the level of trust in certificates issued by that CA. More generally, The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other credential service providers).
Computer Network Exploitation (CNE)	The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Federal Public Key Infrastructure (FPKI)	The FPKI facilitates secure (trusted) physical and logical access, document sharing, and communications across federal agencies, and between federal agencies and outside bodies such as universities, state and local governments, commercial entities, and other communities of interest. To provide trust services, the FPKI uses a set of digital certificate standards, processes, and a mission-critical Trust Infrastructure to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. It uses a security technique called Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure technical non-repudiation and confidentiality.
FPKI Community	The FPKI Community is comprised of government and commercial organizations, which enable trust for interoperable, high-assurance person, entity, or non-person-entity (NPE) identity authentication. For a complete description of the FPKI Community, see Federal Public Key Infrastructure (FPKI) Concept of Operations (ConOps)
Federal Public Key Infrastructure Management Authority (FPKIMA)	The FPKIMA operates, maintains, and manages the FPKI Trust Infrastructure on a day-to-day basis in accordance with the Federal X.509 Certificate Policies and the Certification Practice Statements approved by the FPKIPA.

Term	Definition
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is the FPKI governing body that develops digital-certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incident Management	Process for handling any event that may negatively impact the FPKI Community and/or Relying Parties, and therefore requires immediate attention and resolution (i.e., incident management).
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Problem Management	Root cause analysis with the goal to prevent an incident from reoccurring.
Related External Organizations	Organizations (e.g., vendors, government agencies) the FPKI interfaces with, and depends upon various external organizations but with whom there is no direct relationship.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
U.S. Cert	A partnership between the Department of Homeland Security and the public and private sectors, established to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation.
Unrelated External Organizations	Unrelated organizations are those that are neither in the FPKI Community nor a related FPKI external organization.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix E Acronyms

Acronym	Definition
AA	Agency Application
ACES	Federal Access Certificates for Electronic Services
BAE	Backend Attribute Exchange
CA	Certification Authority
CAB	Certification Authority Browser
CAPI	Cryptographic Application Programming Interface
CIO	Chief Information Officers
ConOps	Concept of Operations
CPWG	Certificate Policy Working Group
CRL	Certificate Revocation List
CSD	Computer Security Division
CSP	Credential Service Provider
CSRC	Computer Security Resource Center
DHS	Department of Homeland Security
EAO	E-Authentication Authorizing Official
EAS	Emergency Alert System
EGCA	E-Governance Certification Authority
EGTS	E-Governance Trust Services
ET	Eastern Time
FBCA	Federal Bridge Certification Authority
FCPCA	Federal Common Policy Certification Authority
FEMA	Federal Emergency Management Agency
FPKI	Federal Public Key Infrastructure
FPKIMA	Federal Public Key Infrastructure Management Authority
FPKIPA	Federal Public Key Infrastructure Policy Authority
FRCA	Federal Root Certification Authority
GSA	General Services Administration

Acronym	Definition
ICAM	Identity, Credential and Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
IdP	Identity Provider
IMP	Incident Management Process
IPAWS	Integrated Public Alert and Warning System
ISC	Internet Storm Center
ISIMC	Information Security and Identity Management Committee
ITL	Information Technology Laboratory
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
RP	Relying Party
SHA	Secure Hash Algorithm
SSP	Shared Service Provider
SSPWG	Shared Service Provider Working Group
TAG	Technical Advisory Board
TWG	Technical Working Group
US-CERT	United States Computer Emergency Readiness Team
WG	Working Group