NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

UNITED STATES NAVY IMPLEMENTATION OF DEPARTMENT OF THE DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI)

by

Christopher J. Michelsen

September 1999

Thesis Advisor:	Rex Buddenberg
Second Reader:	John Osmundson

DTIC QUALITY INSPECTED 4

Approved for public release; distribution is unlimited.

19991022 172

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1999	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE
UNITED STATES NAVY IMPLEMENTATION OF DEPARTMENT OF THE DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI)

5. FUNDING NUMBERS

6. AUTHOR(S)
Michelsen, Christopher J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/ MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

Information assurance (IA) within DoD is becoming an increasingly difficult task as information resources are moving toward a web-based environment. To counter this problem, DoD is mandating that all services implement DoD Public Key Infrastructure (PKI). DoD PKI is part of DoD's defense in depth strategy. It leverages the power of public key cryptography and digital certificates to improve IA. The thesis begins with a presentation of background information on public/private key cryptography and the elements of a PKI. The thesis then discusses those PKI management issues, i.e., CRLs and directories, that an IT manager should consider when implementing a PKI. The thesis then outlines the three areas the Navy should focus on as it implements DoD PKI; specifically PKI implementation strategies, key distribution alternatives, and how to manage change. In response to the first two areas, the author recommends regionalization, based upon the NMCI architecture, smart cards, and biometrics as answers. In response to the third area, the reader is provided with a discussion on managing change as it relates to the implementation of DoD PKI. The thesis is concluded with a discussion of what the Navy and DoD needs to do in order to implement the ideas presented in this thesis.

14. SUBJECT TERMS
Public Key Infrastructure, Public Key Cryptography, Computer Security, and Biometrics

15. NUMBER OF PAGES
141

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

UNITED STATES NAVY IMPLEMENTATION OF DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI)

Christopher J. Michelsen
Major, United States Marine Corps
B.A., Eastern Kentucky University, 1989

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1999

Author: _____
Christopher J. Michelsen

Approved by: _____
Rex Buddenberg, Thesis Advisor

_____
John Osmundson, Second Reader

_____
Dan C. Boger, Chairman
Information Systems Academic Group

ABSTRACT

Information assurance (IA) within DoD is becoming an increasingly difficult task as information resources are moving toward a web-based environment. To counter this problem, DoD is mandating that all services implement DoD Public Key Infrastructure (PKI). DoD PKI is part of DoD's defense in depth strategy. It leverages the power of public key cryptography and digital certificates to improve IA. The thesis begins with a presentation of background information on public/private key cryptography and the elements of a PKI. The thesis then discusses those PKI management issues, i.e., CRLs and directories, that an IT manager should consider when implementing a PKI. The thesis then outlines the three areas the Navy should focus on as it implements DoD PKI; specifically PKI implementation strategies, key distribution alternatives, and how to manage change. In response to the first two areas, the author recommends regionalization, based upon the NMCI architecture, smart cards, and biometrics as answers. In response to the third area, the reader is provided with a discussion on managing change as it relates to the implementation of DoD PKI. The thesis is concluded with a discussion of what the Navy and DoD needs to do in order to implement the ideas presented in this thesis.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. PURPOSE OF RESEARCH 1

B. SCOPE OF THESIS 4

C. THESIS ORGANIZATION 6

II. BACKGROUND 9

A. PRIVATE OR SYMMETRIC KEY CRYPTOGRAPHY 9

B. PUBLIC OR ASYMMETRIC KEY CRYPTOGRAPHY 11
1. Nonrepudiation 12
2. Authentication 13
3. Integrity 13
4. Confidentiality 15
5. Authorization 16

C. PUBLIC KEY INFRASTRUCTURE 18
1. Root Certification Authority (Root CA) 19
2. Certification Authority (CA) 19
3. Registration Authority (RA) 20
4. Local Registration Authority (LRA) 20
5. Directories 20
6. Users 21

III. PKI MANAGEMENT 23

A. ARCHITECTUAL FLEXIBITY 23
1. Subscriber Validation and Enrollment 24
2. Certificates 25
3. Revocation Strategies 27
4. Interoperable Domains 29
5. Certificate Protocol 30
6. Applications 30

B. TRUSTWORTHY OPERATIONS 31
1. Protection Against System Threats 31
2. Trustworthy Components 33

3. Certification and Accreditation 34
4. Warranty and Liability Protection 35

C. AVAILABILITY AND SCALABILITY 36

1. System Back Up and Recovery 36
2. Business Resumption Planning 38
3. Response Times 39
4. Binding Service Level Agreements 40

D. CUSTOMER SERVICE SUPPORT 41
1. Skilled Personnel 41
2. Knowledge Database 42
3. Answers to Queries 43

IV. PKI IMPLEMENTATION STRATEGIES 45

A. THE NAVY PLAN 45

B. DOD PKI TIMELINE 47

C. NAVY ARCHITECTURE 48

1. Navy Marine Corps Intranet (NMCI) 49
a. Wide Area Network (WAN) 49
b. Metropolitan Area Network (MAN) 50
c. Campus Area Network (CAN) 50
d. Operational Area Network (OAN) 50
e. Regional Information Technology Service Center (RITSC) 50
2. Regionalization 51
3. Biometrics 54
a. Proposal One 56
b. Proposal Two 59
c. Proposal Three 60
4. Smart Cards 62

D. KEY DISTRIBUTION 64
1. Key Type 65
2. Physical Key Distribution 67
a. Sustainment 68
b. Ramp-up 69
c. Initial Deployment 70

V. MANAGING CHANGE 71

A. THE CHALLENGE OF CHANGE 71
1. Transitional Change 71
2. Timing 72
3. Enabling Change 73
a. Pace 73
b. Scope 73
c. Depth 73
d. Publicity 74
e. Supporting Structures 74
4. Reaction 74
5. Trigger Events 75
6. Mindsets 76
a. Assembly 76
b. Conventional 76
c. Amended 76
d. Evaluative 77
7. Managing Mindsets 77

B. ENVISIONING CHANGE 78
1. Vision 78
2. Vision Statement 79
3. Visionary 80
4. Commitment to a Vision 81
a. Communication 81
b. Boundary Testing 81
c. Sign-on 82
d. Celebration 82
5. Alignment 83
6. Dissatisfaction 83

C. IMPLEMENTING CHANGE 85
1. Change Participants 85
2. Implementation Problems 86
a. Time 86
b. Problem Areas 86
c. Coordination 86
d. Competing Activities 87
e. Capabilities 87
f. Training 87
g. Outside Factors 87

3. Tactical Implementation Steps 87
a. Analyze the Organization and Its Need for Change 87
b. Create a Shared Vision and Common Direction 88
c. Separate from the Past 88
d. Create a Sense of Urgency 88
e. Support a Strong Leader Role 88
f. Line up Political Sponsorship 88
g. Craft an Implementation Plan 89
h. Develop Enabling Structures 89
i. Communicate, Involve People, and Be Honest 89
j. Reinforce and Institutionalize Change 89
4. Basic Concepts of Organizational Change 89
a. Managing the Political Dynamics Associated with Change 91
b. Motivating Constructive Behavior in the Face of the Anxiety Created by the Change 91
c. Actively Managing the Transition State 91
5. Types of Organizational Change 92
6. Organizational Frame Bending 93
a. Initiating Change 93
(1) Rationale 94
(2) Stakeholders 94
(3) Values 94
(4) Performance Objectives 95
(5) Organizational Structure or Processes 95
(6) Operating Style 95
b. Content of the Change 95
c. Leading Change 96
(1) Distinctive Behaviors 96
(2) Ability to Create a Sense of Urgency 96
(3) Guardianship of Themes 96
(4) A Mix of Styles 96
d. Achieving Change 97
7. Developing Change Processes 99

D. THE RECIPIENTS OF CHANGE 101
1. Reaction to Change 101

E. CHANGE AGENTS 107

VI. CONCLUSIONS 115

A. THESIS SUMMARY 115

B. THE TRANSITION 115

1. Primary Research Question One 116
a. PPBS 116
b. Software Development 116
c. Standards 117
d. Customer Service 117
e. Education 118
2. Primary Research Question Two 118
a. Implementation Strategy 118
b. Policy 119
3. Primary Research Question Three 120

C. RECOMMENDATION FOR FUTURE RESEARCH 121

LIST OF REFERENCES 123

INITIAL DISTRIBUTION LIST 125

ACKNOWLEGEMENT

The author would like to especially thank Professor Rex Buddenberg for his guidance and encouragement. Without his assistance, this thesis would not have been possible.

A special thanks goes to my loving wife, Kelly, and my two wonderful children, Jessica and Samuel, for their patience and unwavering support. When times were tough, they were always there.

The author would finally like to thank Polly and Jerry Michelsen, a.k.a. Mom and Dad. Without your outstanding upbringing and support none of this would have been possible. Thank you!

I. INTRODUCTION

A. PURPOSE OF RESEARCH

The Internet is growing at an amazing rate. Most studies in to the size of the Internet are outdated soon after they are published. As a result of the growth of the Internet, people are progressively moving from a paper driven society to a digital one. This digital society is also a networked society. Due to the increases in technology, it is becoming easy to transmit data, voice, or video over the Internet. In addition, the Internet gives anyone the ability to digitally link themselves to any other computer, web server, or router on the Internet. The problem with the Internet is that it is open to anyone and its internal security mechanism is based on the simple principle of trust. That is trust that people will not misuse it and that all users will respect the privacy of others. Unfortunately, this trust mechanism has not proven sufficient to meet the needs of the average user, much less the Department of Defense (DoD). Anyone on the Internet can download software that gives them the ability to sniff packets as they pass over the net or hack into a web server or router. The technology is out there and it is freely available to anyone willing to put in the time to learn how to use it.

In order to increase the security of the Internet, various security protocols have been developed. The prevailing protocol in use today is link encryption. A link is a serial data circuit connecting two machines [Ref. 1]. Link encryption consists of encryption applied to an entire transmission between two hosts [Ref. 2]. It has the benefit of hiding the transmission's characteristics, thereby enhancing traffic flow integrity and preventing traffic flow analysis. Traffic flow analysis is the obtaining of information through observing characteristics of the transmission itself, i.e. source, destination,

frequency, and size of transmission [Ref. 2]. The problem with link encryption is that there exists no legal or physical way to ensure your transmission was not intercepted, modified, or diverted. At each link or node in the network the transmission must be decrypted, link encryption removed, so that the router can see the datagram header and properly route the transmission [Ref. 2]. It is re-encrypted again before it is sent to the next link in the network. Therefore, link encryption does not provide "complete" confidentiality. If all links are not physically secure, then there exists the possibility that someone could view, alter, or reroute a transmission. Link encryption provides a good defense against traffic flow analysis, but is susceptible to a physical security breach at any one of the links in the network. In addition, some feel link encryption is uneconomic because it essentially secures the links, but not the data flowing over them. To counter these weaknesses end-to-end encryption was developed.

In contrast to link encryption, end-to-end encryption provides encryption and decryption only at the source and destinations hosts [Ref. 2]. This ensures the confidentiality of the transmission. However, it does nothing to hide the header of the datagram. Therefore, end-to-end encryption is susceptible to traffic flow analysis. Only a network with a combination of end-to-end and link encryption can one be sure of confidentiality and traffic flow integrity. However, end-to-end encryption can provide authentication, nonrepudiation, privacy, authorization, and data integrity [Ref. 3]. Public key cryptography is the technical mechanism that enables end-to-end encryption. An example will illustrate the power, usefulness, and security of public key cryptography.

Figure 1-1 shows a notional network with the following properties: sensors, database, and decision support system (DSS). In the example, the unmanned sensors pick

up information, i.e., weather conditions, a still picture of an intersection, energy consumption of a reactor, etc., and, by program, prepare the information for transmission.

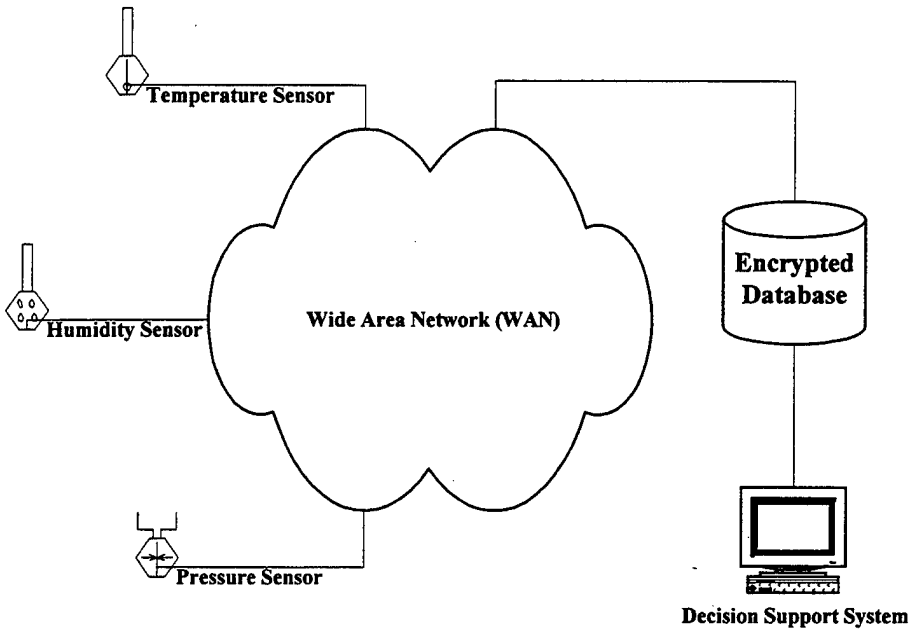


Figure 1-1. The Power of Public Key Cryptography

They do this by creating a digital signature, this will be discussed in Chapter II, and encrypt the transmission with the recipient's public key and the sensor's private key. The information can then flow across public networks until it reaches its initial destination a database. The database management system (DBMS) knows how to store the information and does so in its encrypted form. When needed, the DSS extracts the information from the database and decrypts the information with its private key and the sensor's public key. What this example truly shows is that the information is completely secure all the way from the origin, through the network, into database, and finally to the

secure DSS. And neither any of the links in the network nor the database required securing; a huge cost savings!

Ninety-five percent of all DoD does operates over public networks [Ref. 4]. With this being the case, the DoD has a strong need to ensure its transmissions are secure. All of DoD's classified transmissions utilize at a minimum a symmetric encryption protocol. DoD's problem lies with its sensitive but unclassified (SBU) and below information. It currently travels in the "clear" over primarily public networks. In the world, there is an increasing importance being placed on information. And information superiority is the name of the game on the battlefield today. This being the case, DoD must increase its security posture in order to protect its valuable network resources and information. To accomplish this task, DoD is going to institute end-to-end encryption on all of its networks and on all SBU and below information passed over its Intranets and the Internet. In order to accomplish end-to-end encryption, DoD is mandating the establishment of a DoD Public Key Infrastructure (PKI).

B. SCOPE OF THESIS

There are two primary research questions the author set out to answer in response to DoD's mandate that all services implement DoD PKI:

- How should the Navy organize its public key infrastructure in order to most efficiently and cost effectively implement DoD PKI?
- How will the Navy distribute key pairs to 365,108 active duty, 196,986 ready reserve, and 195,058 civilian personnel [Ref. 5]?

These questions helped the author focus his research efforts and incrementally answer the questions as presented in the thesis. While developing answers to the two

primary research questions, the magnitude of the change became apparent. As a result of this discovery, a third research question, which required further examination, presented itself:

- How does the Navy manage the change-related issues surrounding the implementation of DoD PKI?

The body of the thesis was built around these three research questions. In the course of doing research the author discovered many important issues that can affect the Navy's implementation of DoD PKI, but are beyond the specific scope of this thesis.

One example is the Navy Marine Corps Intranet (NMCI), formerly the Navy Wide Intranet (NWI). Whereas NMCI is not a requirement for the Navy's implementation of DoD PKI, it would provide an efficient architecture for DoD PKI to attach to. There are also some funding, and therefore political, discussions surrounding NMCI. Both of these issues are important to the Navy's implementation of DoD PKI, but are outside the research focus of this thesis.

An additional issue, which was not studied, was the personnel requirements surrounding the Navy's implementation of DoD PKI. Large numbers of Sailors and civilians will be required to operate and maintain the system. In addition, a large number of Sailors and civilians will be required to train all personnel throughout the Navy on DoD PKI. These personnel need to be sourced, funded, and trained. Individual training standards need to be established for the trainers, maintainers, and operators as well.

C. THESIS ORGANIZATION

There are six chapters, which outline the results of the author's research. The first three chapters provide background information for those readers unfamiliar with public

key cryptography, PKI management, or DoD PKI. They set the stage for the remainder of the thesis. The next two chapters answer the three fundamental questions and are the core of the research. The following paragraphs provide a summary of the chapters:

- Chapter I – Introduction. This chapter outlines the purpose of the thesis, scope of the thesis, and organization of the thesis.
- Chapter II – Background. This chapter provides a brief overview of public and private key cryptography, defines PKI, and discusses DoD PKI and what it means to DoD and specifically to the Navy.
- Chapter III – PKI Management. This chapter provides the reader with background information surrounding the management of a PKI. Included are those issues which managers must concern themselves with if they decide to implement a PKI. Problem areas are emphasized.
- Chapter IV – PKI Implementation Strategies. This chapter answers the first two research questions. It provides a wide array of options and identifies the author's preference. It considers regionalization, biometrics, and DMDC as possible alternatives.
- Chapter V – Managing Change. This chapter answers the last research question. The issues surrounding change are often overlooked. This chapter provides a comprehensive overview of those issues managers must consider when instituting change. It provides specific examples for the Navy with regard to their implementation of DoD PKI.

- Chapter VI – Conclusion. This chapter provides concluding comments, outlines what the Navy needs to do in order to implement the ideas in this thesis, and discusses potential areas for future research.

THIS PAGE INTENTIONALLY LEFT BLANK.

II. BACKGROUND

The first step toward analyzing the Navy's implementation of DoD Public Key Infrastructure (PKI) is to understand the concepts involved. This chapter will provide the reader with background information regarding public key infrastructures and public and private key cryptography. This chapter is only intended as an overview and the reader is referred to the list of references for a record of sources that contain a more expansive coverage of the topics.

A. PRIVATE OR SYMMETRIC KEY CRYPTOGRAPHY

Currently, the Navy uses symmetric or private key cryptography to secure its information. Symmetric key cryptography utilizes the same key at both ends of the transmission. The key is able to encrypt and decrypt information. Figure 2-1 is an example of symmetric or private key cryptography.

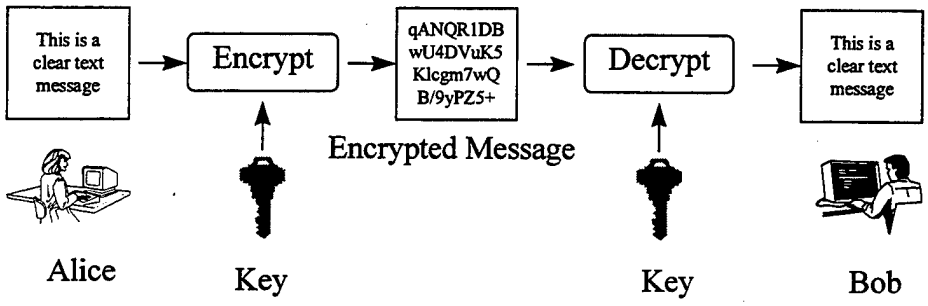


Figure 2-1. Symmetric or Private Key Cryptography [From Ref. 5]

The system is very secure. One problem lies with key distribution. In order to utilize private key cryptography, all users must have a copy of the key and confidentiality of the key must be assured. This becomes a large logistics' problem with large organizations like the U.S. Navy and DoD. The keys must be pre-staged in order for the correct keys to be on hand when required. This is very similar to DoD's

Communications Security Materials System (CMS). Another problem is key security or confidentiality. If just one of the potentially thousands of keys are lost, then the whole system becomes vulnerable. The distribution problem becomes immense again, as new keys must be distributed to everyone. With private key cryptography, there is no way to know whom a message came from unless "only" two people have the key. In other words there is no means of authenticating communicating parties. There is also no means of enforcing non-repudiation, which is the sender can not deny having sent the message. Symmetric key cryptography is also vulnerable to the man-in-the-middle attack, see Figure 2-2. This is where someone gains a copy of the key, intercepts the message from the sender, and forwards the message to its intended recipient. This is all done without the sender or recipient's knowledge.

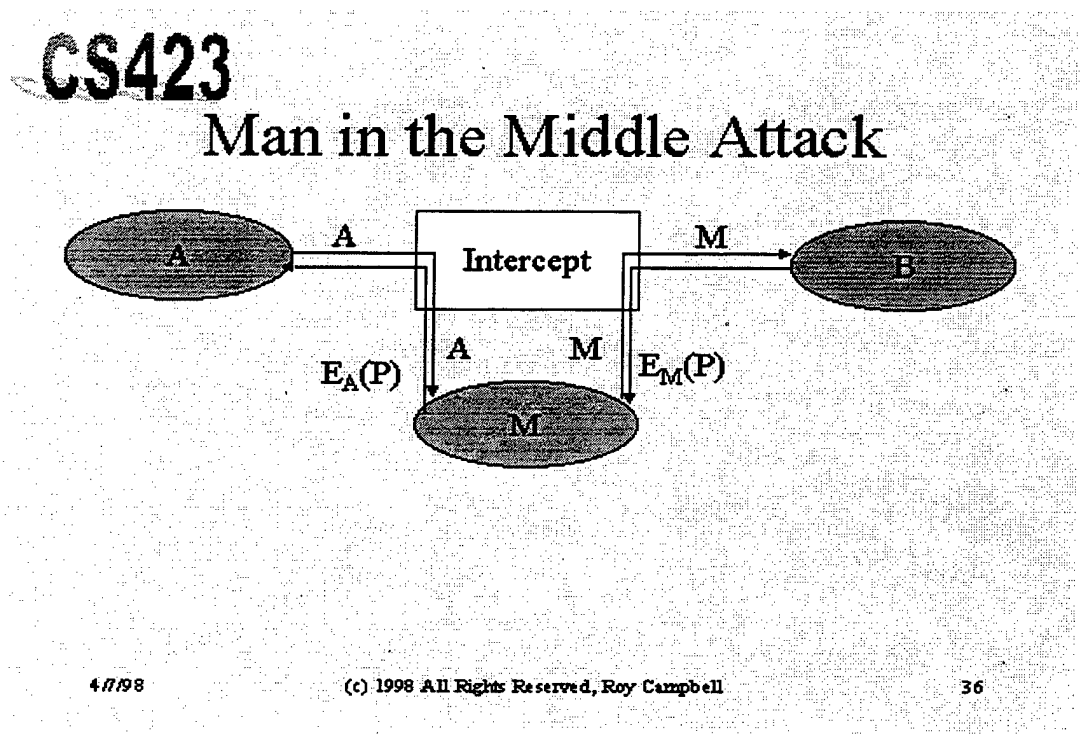


Figure 2-2. The Man-in-the-Middle Attack [From Ref. 3]

Due to the complexity and logistics involved, symmetric keys are not usually passed down to the individual user. They are utilized at the command or unit level. Therefore, there is no end-to-end encryption. It is simply link encryption. Each link throughout the network decrypts and then re-encrypts the message as it passes through the network. If only one operator is less than honest, then they could view the traffic going across the network. The security chain is only as strong as its weakest link. And the human operator is the weakest link in symmetric key cryptography. To prevent or solve all of these problems public key cryptography has evolved.

B. PUBLIC OR ASYMMETRIC KEY CRYPTOGRAPHY

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone else's public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Figure 2-3 describes the basics of public key cryptography.

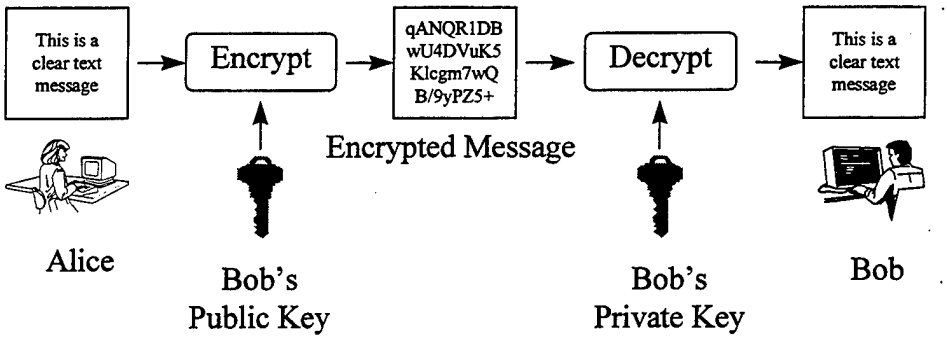


Figure 2-3. Public or Asymmetric Key Cryptography [From Ref. 5]

The idea behind public key cryptography is that only the private key can decrypt the public key and only the public key can decrypt the private key. These facts make the system secure. This type of security provides some added benefits:

1. Nonrepudiation

Nonrepudiation is when the sender of a message can not deny having sent a message. This is accomplished when the sender signs a message with his or her private key. This is called a digital signature. Since the sender is the only person to have access to the private key and only the public key can decrypt the private key, the message must have come from the sender. Nonrepudiation protects against the sender saying, "I didn't send that message." The recipients response is, "Yes, you did. You signed it with your private key." Figure 2-4 shows how to digitally sign a message.

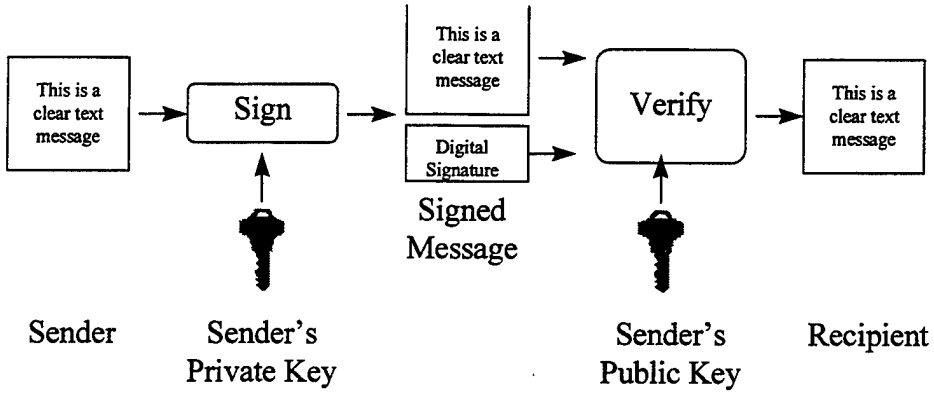


Figure 2-4. Signing a Message [From Ref. 5]

2. Authentication

The process for authentication is the same as nonrepudiation. In symmetric key cryptography, if there are more than two keys (there usually are), then there is no assurance who "actually" sent a message. Did it come from Bob or Alice? Public key cryptography answers this question with the digital signature. Again, because the owner of the private key is the only one with access to it, any message encrypted with the private key must have come from them.

3. Integrity

Data integrity is an important concern in today's networked world. What assurances does the sender or receiver of a message have that it was not altered en route? A digital signature could be used so that if some one altered the message the recipient would detect it. However, encrypting a message with the senders' private key is very computationally slow. To speed up the process, public key cryptography utilizes a hashing function. This is a mathematical function that takes any sized message and compresses it down to a consistently small form. Some liken this compression to a fingerprint. This fingerprint, in technical language, is called a message digest. Every

document possesses a different fingerprint. If only one bit of the message is changed, the hash function would produce a completely different fingerprint. Hashes are one way only. Once a message is hashed there is no way to retrieve the message from the hash. How does this answer the problem of data integrity? The sender of the message sends a copy of the message unaltered called plain text, to the recipient. In addition, he sends a copy of the message's hash, which has been encrypted with the sender's private key, digital signature. When the receiver receives the hash and the plain text message; they decrypt the hash and hash the plain text. The receiver then compares both hashes. If they match, the message was not altered en route. This prevents the-man-in-the-middle from altering transmissions. Figure 2-5 illustrates data integrity through use of the hashing function.

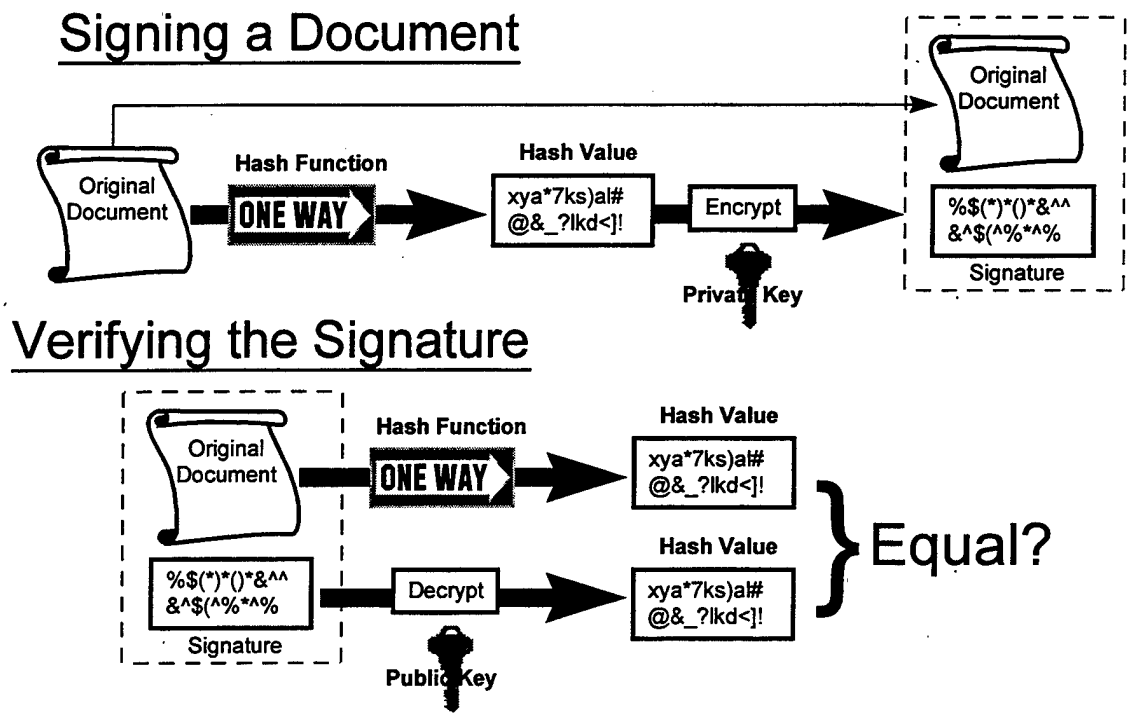


Figure 2-5. Data Integrity [From Ref. 5]

4. Confidentiality

In order to ensure the man in the middle can not view the plain text message, confidentiality is needed. This is can be accomplished by encrypting the message with the recipient's public key. By doing this, only the recipient, using their private key, can decrypt the message. This process, as stated earlier, is computationally slow. In order for the process to be expedited the concept of session keys was born. A session key is a symmetric or private key that both parties agree to utilize. The idea is that the sender and recipient will utilize public or asymmetric key cryptography to exchange session keys. They will then utilize secret or symmetric key cryptography to exchange information, pass messages, etc. The reason this process is utilized is that secret key cryptography is not computationally slow, therefore confidentiality services can be expedited. Figure 2-6 shows how confidentiality is leveraged using session keys.

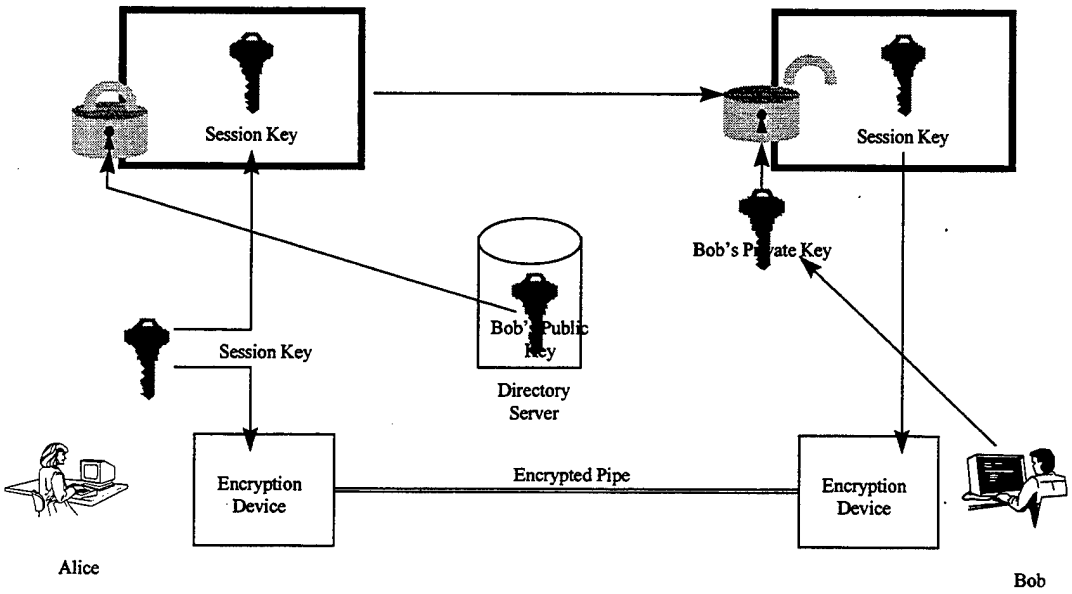


Figure 2-6. Confidentiality via Session Keys [From Ref. 5]

5. Authorization

Authorization deals with privileges. These privileges are imbedded into digital certificates; these will be discussed below. Utilizing a properly issued credential on a digital certificate an individual can use his key pair to evoke certain privileges. There are two key ideas to authorization. The first is having an infrastructure in place to issue credentials, in this case digital certificates. And second, there must exist applications capable of utilizing digital certificates to authorize certain persons, certain privileges, based on their public key pair. Figure 2-7 shows an example of how authorization works.

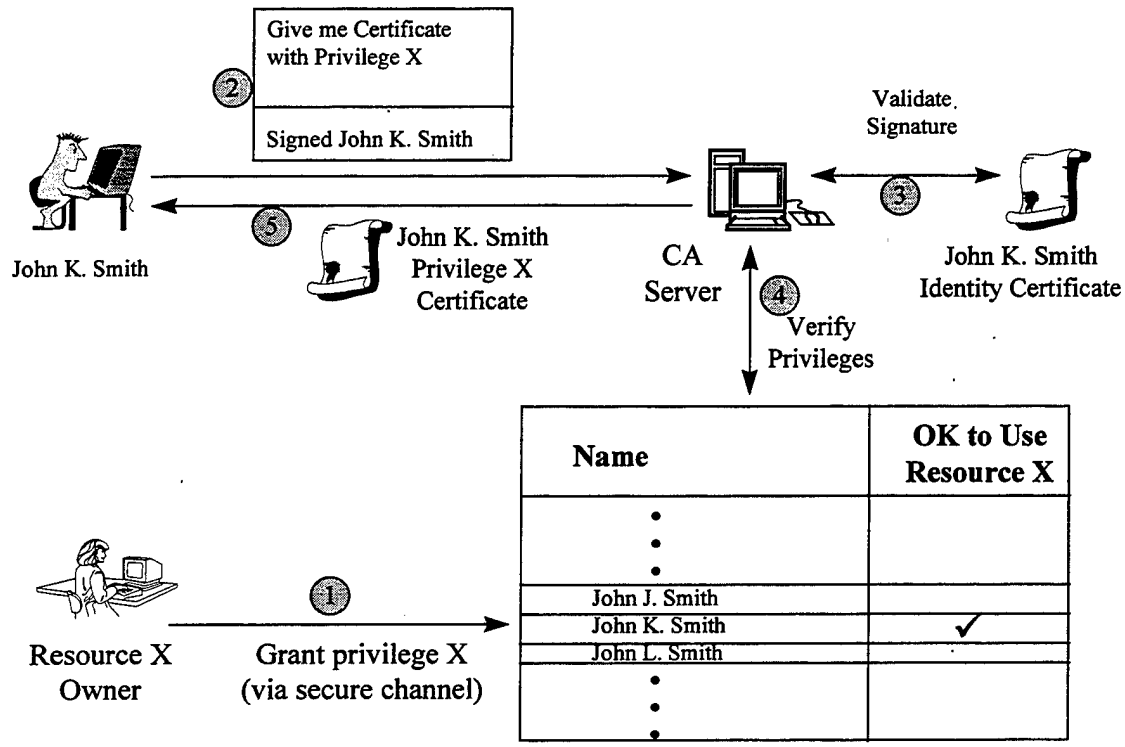


Figure 2-7. Authorization [From Ref. 5]

The most secure means of communication, but computationally slow, is to encrypt your plain text message and hash twice; once with the recipient's public key and then with the sender's private key. This ensures the following:

- The sender is who they say they are - authentication.
- The recipient is the only one who can read the message - confidentiality.
- The sender can not deny sending the message - non-repudiation.
- The message was not altered in transmission - integrity.
- The sender was allowed a certain privilege – authorization.

One of the crucial elements of public key cryptography is trust. This is because we must trust that the public keys we utilize actually belong to whom they say they do. But what assures this? The answer to this question is digital certificates. "The main purpose of the digital certificate is to ensure that the public key contained in the certificate belongs to the entity to which the certificate was issued." [Ref. 2] To certify people to their public keys, digital certificates are used. A digital certificate is a kin to a trusted third party certifying that a person is who he says he is. In addition, the trusted third party binds this confirmed identity to the person's public key. The trusted third party accomplishes this by issuing a digital certificate to the person that says just that. To ensure authenticity of certificates and reduce fraud, the trusted third party digitally signs the certificate with its private key. These certificates vouch for the identity of its holder. The key idea with digital certificates is that if the third party certificate or "voucher" is trusted, then the certificates they issue are trusted as well. Who are these "trusted third parties"? How are certificates issued? How are public keys and their certificates

managed? The answers to these questions are found in the infrastructure that supports them.

C. PUBLIC KEY INFRASTRUCTURE

The five benefits of public key cryptography, outlined earlier, will greatly improve the Navy's information assurance (IA) security posture. However, there must exist an infrastructure for these public keys and digital certificates to rest upon. This is where DoD PKI comes in. A public key infrastructure is "...the framework and service that provides for the generation, production, distribution, control and accounting of public key certificates and provides the critically needed support to application and providing confidentiality and authentication of network transactions as well as data integrity and non-repudiation." [Ref. 6]

A PKI is made of elements required for the secure, simple access of public keys and public key cryptography. These elements are:

- Root Certification Authority (Root CA)
- Certification Authority (CA)
- Registration Authority (RA)
- Local Registration Authority (LRA)
- Directories
- Users

These elements are linked together as seen in Figure 2-8.

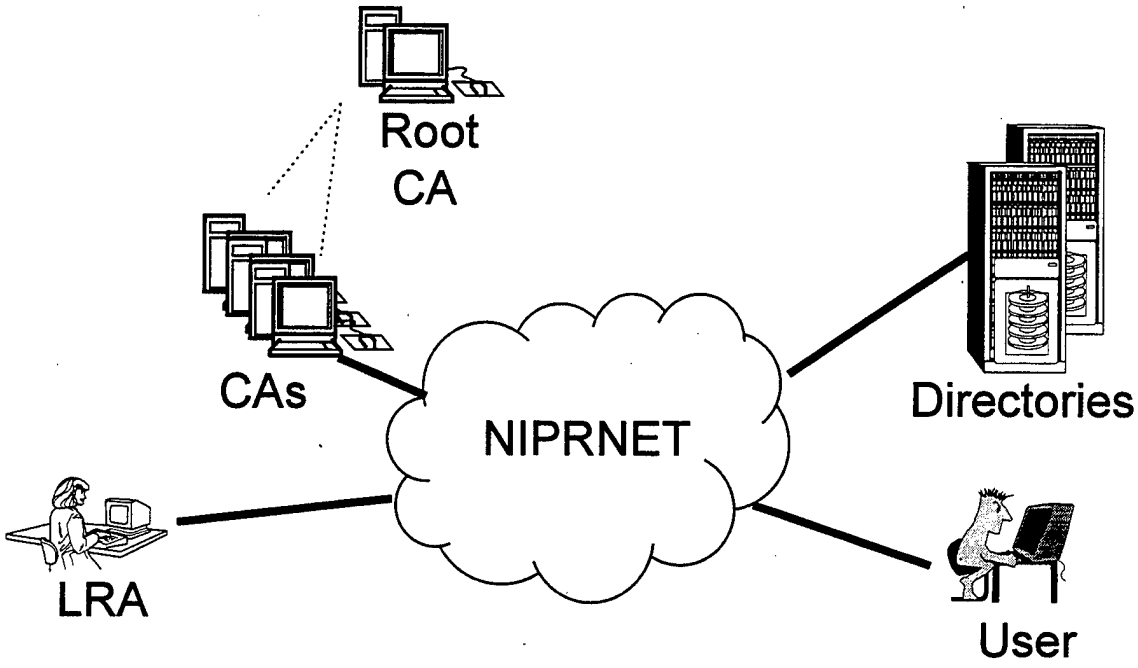


Figure 2-8. Elements of DoD PKI [From Ref. 5]

1. Root Certification Authority (Root CA)

The root CA is the basis for the PKI. Its private key must be very securely safeguarded. If it were to be compromised, all certificates based upon it would be compromised too. In order for it to stay safe, multiple officials must be present during its use and it is kept offline to prevent unauthorized access. This is analogous to the bank vault where each bank officer only knows part of the combination, but no one knows all of it. The release of nuclear weapons works the same way. The root CA issues the CAs' certificates and signs them with its private key, vouching for their identity and trustworthiness. The DoD PKI Root CA is run by NSA and located in Finksburg, MD.

2. Certification Authority (CA)

The CAs issue certificates to RAs, LRAs, and users. They are responsible for putting the public keys in the directories and managing certificates. This management consists of revoking certificates, creating certificate revocation lists (CRLs), sending

CRLs to the directories and renewing certificates [Ref. 5]. Currently the DoD is planning on having two CAs, one in Denver, CO and the other in Chambersburg, PA. Alternatives to this organization are discussed in Chapter IV.

3. Registration Authority (RA)

RAs are responsible for registering LRAs. The Navy tentatively plans to have approximately 1,800 LRAs. Alternatives to this organization are discussed in Chapter IV. Currently there is only one RA in the Navy located at the Director, Communications Security Material System (DCMS). Alternatives to this organization are also discussed in Chapter IV.

4. Local Registration Authority (LRA)

LRAs are responsible for registering users. Users are required to prove their identity using their DoD ID card. This creates a trust model. The LRA trusts the ID card, the ID card issuer trusts a person's military records, and military records are initiated with your birth certificate. The whole system can be penetrated by a person gaining a fraudulent identity via a fraudulent birth certificate. Once the identity is verified, the LRA then registers the user and shows them how to generate their key pair and get their certificate from the CA.

5. Directories

A key element of any PKI is directories. Without them a PKI lacks usability. The directory stores all current public keys and the current certificate revocation list, which is the list of all revoked, but not yet expired certificates.

6. Users

It is envisioned that all DoD personnel, both military and civilian, will be issued certificates and a key pair. The user is responsible for ensuring his private key remains confidential. Currently the user is the weakest link in DoD PKI.

There are many details to the operation of a PKI that were not covered in this chapter. However, the essential elements of public and private key cryptography and PKI were presented. The reader should now have sufficient background information in order to understand and leverage the information contained in the remaining chapters of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK.

III. PKI MANAGEMENT

In order to fully appreciate the magnitude of DoD PKI and the changes and challenges that it represents, a thorough coverage of PKI management is necessary. PKI management consists of those actions related to the proper administration and management of the three major components of PKI:

- Technology – Public key cryptography, digital signatures, certification authority software, and certificates.
- Policies, procedures, and practices – Decisions made about how things are done and what is required by a particular CA.
- Operations – The actual systems and staff that run the CA and enforce policies and procedures. [Ref. 7]

This chapter will present those issues the information technology (IT) professional should address in order to implement a workable and livable PKI solution. The focus of the chapter will be on DoD PKI and where appropriate, recommended courses of action for DoD and the Navy will be provided. This chapter will break down PKI management issues by its operational mandates:

- Architectural Flexibility
- Trustworthy Operations
- Availability and Scalability
- Customer Support and Service [Ref. 8]

A. ARCHITECTURAL FLEXIBILITY

Architectural flexibility addresses those PKI management issues that deal with:

- Subscriber Validation and Enrollment
- Certificate Contents
- Revocation Strategies

- Interoperable Domains
- Certificate Protocol
- Applications [Ref. 8]

These are some of the most important issues to the IT manager, especially as he contemplates a PKI implementation strategy.

1. Subscriber Validation and Enrollment

Subscriber validation and enrollment protocols are those means that a user has to validate his identity and register for a certificate. There are basically two types of validation and registration, remote and in person. Currently, DoD only supports in person verification of identity by a certificate management authority (CMA), most likely an LRA administrator, or an agent approved by the CMA for class III and IV certificates [Ref. 9]. The issue that the IT manager must consider is how industry is conducting validation and enrollment. Currently, industry is validating and enrolling subscribers remotely [Ref. 8]. If DoD intents to be interoperable with industry, how can this be accomplished when both groups have separate and distinct validation and enrollment policies? In order for industry and DoD to truly leverage the power of PKI, the infrastructure needs to operate under a homogeneous enrollment and validation policy [Ref. 8]. The author feels a remote shared secret enrollment and validation methodology or a biometrics authentication scheme could answer this problem. In addition, it would alleviate the need for large numbers of personnel to support the in person verification and enrollment process. This idea will be amplified in Chapter IV.

2. Certificates

Certificates are the heart of any PKI. They are what subscribers use to trust the identity of another subscriber or authenticate themselves to a system. IT managers must make decisions early on as to what information a certificate will contain. There are several choices here. One option is for certificates to contain only the absolute minimum information necessary to uniquely identify a person and bind that person to their public key. This is the DoD plan for identity and encryption certificates [Ref. 6]. The certificates will contain the following information:

- Version Number
- Issuer's Name
- Serial Number
- Individual's or Entity's Name
- Public Key
- Validity Period [Ref. 6]

Attributes and privileges are additional information that can be amended to a certificate that identifies a person or device as possessing certain qualities. These qualities can be used as a basis for granting or disallowing a person or device certain permissions. The reason to add attributes to a certificate is robustness and flexibility. For example, a person or device's certificate could state that he or it had nuclear launch permission. If a Boomer CAPT or launch system received a digitally signed message from the President stating to launch nuclear missiles and the CAPT or launch system could verify the signature with the President's public key, then the whole launch cycle could be expedited. The reason not to issue attribute certificates is complexity and management.

It takes a lot of additional overhead to manage who has what attributes and when they should be revoked, upgraded, or downgraded. Initially, DoD does not plan to issue attribute certificates. DoD's plan to create a bare bones certificate should ensure interoperability though. However, DoD has left room in their plan should they desire to add attributes at a later date. There is another option the IT manager must consider though. And that is a more robust certificate with more information fields. An example will help illustrate this point. The Internet is moving toward web based communications. In order to leverage that power, it might be necessary to put information that represents the business environment into the certificate. For example, assume that access to information is segregated by organization, i.e. CINCPACFLT, SPAWAR, N3, N4, N6, etc. The operations personnel (N3) only need access to operations data, the logistics personnel (N4) only need access to the logistics data, but the CNO needs access to operations, logistics, medical, weapons, etc. This could be accomplished by simply adding organization (N3, N4, or CNO) to the operations Officer, logistics clerk, or CNO's certificate. Whereas limiting certificate contents does have the advantage of interoperability, it does restrict robustness and this is an issue the IT manager, at the N6 (CIO) level, must consider [Ref. 8].

Another option exists where the IT manager can use bare bones identity certificates and access control lists (ACLs). The ACLs would contain the privileges or attributes and they could only be activated if the identity certificate was recognized by the ACL. The disadvantage to this process is that someone has to manage the ACLs, but this could be done by an application on the desktop. ACLs support the interoperability process stated earlier.

3. Revocation Strategies

Certificate revocation is a vitally important function in PKI management. When a certificate expires at its expiration date, users know, because their applications will not honor them. However, if a certificate's private key has been compromised or a subscriber has used his certificate in a fraudulent way it must be revoked immediately. For these reasons, certificate revocation lists (CRLs) were established. CRLs list all those certificates that have been cancelled, for whatever reason, prior to their natural expiration date. When a revoked certificate reaches its natural expiration date, it falls off the CRL.

There are several ways a user can get access to a CRL. The first option is that before utilizing a certificate a user could log on to a web site and check the certificate's status. This option seems to have a lot of overhead, especially time. This is especially true when the user is at the end of a long "delay pipe," i.e., deployed. Does every user want to look up every certificate each time he uses it? The author thinks this will lead people not to use certificates or to not look up their validity due to the time and inconvenience involved.

The next method is for CAs or RAs to send the CRLs out to all of its subscribers on some sort of regular interval. This could be immediately, hourly, daily, weekly, etc. The problem with this approach is that each time the CA or RA sends out the CRL, it will become bigger and bigger. This is because the CA or RA are always sending the entire version out in case someone is a new subscriber or someone has been off line for awhile. This will clog the network with CRLs. It could really slow things down. This author

feels it will cause people not to use certificates and will cause them to see PKI in a bad light.

The author feels there is a preferred, third option. The idea is very similar to the way virus definitions are updated on your computer. An example will illustrate the solution better. As a new user you are required to retrieve your certificate from the CA with your personal identification number (PIN). As part of the process the CA could require you to download the current version of the CRL. At the same time it would require you to look up your certificate to show you that, it is in fact current and not revoked. This is a subtle way of showing people how to look up a certificate without putting them in the "tutorial mindset." Then each time the person logs onto the Internet his CRL application would send a simple request to the CA's CRL server requesting the current CRL status. If the CRL has been updated, the application will prompt the subscriber to download the latest version. However, because the CA's CRL server would know what version you currently had, it would only send you what you needed to become current. This would significantly reduce the amount of CRLs on the network. Another variant of this idea would be to require a sub-set of or all (very time consuming) users to update their CRLs before they could utilize their public or private key over the network. New technology would have to be developed in this case.

DoD currently plans to utilize CRLs and on-line verification. It is concerned over the scalability of on-line verification and standards support [Ref. 6]. The other problem with on-line verification is the need to maintain on-line repositories in addition to directories. This could lead to cost and personnel problems.

The problem with all the options listed above is that industry CRL methodologies are very immature, not well defined, and have yet to be broadly deployed [Ref. 7]. To that end, the author believes that CRLs can be a showstopper for DoD PKI. The more work the user has to do to utilize what PKI can offer, the less likely he is going to utilize the tools. To the greatest extent possible, PKI needs to operate beneath the scenes, transparent to the subscriber. DoD needs to form a partnership with industry and help define the open standards for all to follow.

4. Interoperable Domains

Interoperable domains are what were alluded to earlier as interoperability. This is a very important factor for the IT manager. Unless the premise of the PKI is for internal use only, then plans must be made to ensure interoperability. To that end there are four scenarios DoD PKI must consider

- Government-to-government
- Government-to-industry
- Government-to-citizens
- Intra-government [Ref. 8]

This may seem like a trivial issue, but is of concern to a great many people. Right now DoD will not issue an identity certificate to someone who is not a U.S. citizen or employed in or by the armed services. How then is DoD going to utilize PKI with contractors and foreign companies, NATO forces, or even our enemies (i.e., spies or during treaty negotiations)? The answer to one of these questions is external certification authorities (ECAs). ECAs will be established so that the trust placed in their certificates is comparable to that placed in DoD certificates. This is analogous to third party

embassies during treaty negotiations, i.e. Switzerland at the end of World War II. DoD CIO will approve ECAs. It seems that this process could be made easier if DoD would publish a list of requirements for external CAs to follow. This list would state what public citizens, industry, NATO, and fellow U.S. government agencies and departments would need to do in order for DoD PKI to recognize their CA. Once their CA is recognized as compliant, then both groups could cross certify each other's CA. This is going to be a big problem in DoD for some time to come. DoD is moving very fast with PKI and their efforts are to be lauded, but if they work faster than the standards bodies, there could be a lot of reworking later on. Therefore, it is imperative that DoD PKI gets involved early with the PKI open standards being discussed now.

5. Certificate Protocol

The leading certificate protocol in use today is X.509v3 (version 3). It has been nearly universally accepted as the certificate protocol of choice in PKIs. The DoD has chosen this standard to be the one that will be implemented in DoD PKI. This has been an excellent choice and should ensure interoperability with almost every other PKI in the future. Ref. 9 provides amplifying information with regards to X.509 and DoD's use of it.

6. Applications

Cryptographically aware applications are what make a PKI valuable. A PKI can have the world's best infrastructure, but without cryptographically aware applications to leverage the power of PKI, the PKI is useless. This is currently the problem with DoD PKI and requires a lot of attention if DoD ever expects DoD wide acceptance of PKI. Depending on the application, SPAWAR, PMW-161 has published a lot of work-arounds

in order to help current DoD PKI subscribers to utilize DoD certificates with some cryptographically aware applications. This type of mentality, that of work-arounds, will not work with the common user. PKI must be nearly transparent to subscribers or they will not utilize it. This is where IT managers need to focus a significant portion of their energies in the future.

B. TRUSTWORTHY OPERATIONS

Trustworthy operations deals with those issues the IT manager should focus on that will ensure a smooth functioning PKI now and into the future. These issues consist of protection against system threats, trustworthy components, certification and accreditation, and warranty and liability protection [Ref. 8].

1. Protection Against System Threats

System threats come from three areas: internal, external, and natural disaster. Internal threats consist of those deliberate and accidental actions or lack of action by the system's personnel [Ref. 8]. Deliberate actions can consist of an employee deliberately creating a hole in the firewall or creating fraudulent certificates. Accidental actions can take the form of personnel misconfiguring hardware or not following procedures. The IT manager must ensure that standard operating procedures (SOPs) are in place that will mitigate any accidental threats or mistake. He should also closely screen his employees, prior to hiring, and create checks and balances where vital systems are concerned. Training of personnel is critical to prevent "mistakes." This training can be quite expensive and time consuming. The author feels that DoD will be hard pressed to staff the Root CA, CAs, and RAs with uniformed service members, because of their lack of continuity at a particular site. Training is a continuous process and the service members

have outside commitments other than their normal daily responsibilities, i.e. rifle range, mess duty, morning PT, or being pulled early from an assignment for recruiting duty.

External threats can be labeled structured or non-structured. A non-structured threat is an individual hacker, i.e., the 13-year old at home. Structured threats take the form of organized hacking groups or full-scale National attacks. Proper hardware and software configurations, intrusion detection, and SOPs should address the individual hacker and the hacking group [Ref. 8]. The author feels a determined outside government, depending on the scale of the attack, could definitely bring down or seriously disrupt PKI services. Computer security is just not a mature enough mechanism in the face of a dedicated National attack. Regardless, these are issues the IT manager must address.

Due to DoD PKI's reliance on the Internet, there are only a few issues an IT manager can address when it comes to natural disaster preparedness. The facilities that house the Root CA and the CAs must be hardened against flood, earthquake, tornado, etc. There needs to exist depth in communications and power. Connectivity to the Internet must pass through multiple Internet Service Providers (ISPs) [Ref. 8]. If one goes down, the system should still be able to function through the secondary or tertiary ISP. If main power goes down, diesel or photoelectric power needs to take over. A lot of these issues are at the highest IT manager level, but to some degree, apply to every IT manger. In essence, an IT manager is his own logistics officer when it comes to his system's resources.

2. Trustworthy Components

The trustworthy components are systems, people, and policies and practices. These components, if chosen properly, will provide some stability for the system or in this case, DoD PKI.

The systems components consist of cryptographic modules, hardware, and software. The cryptographic modules are an example of success in DoD PKI. Early on, an internationally recognized standard was chosen, Federal Information Processing Standard (FIPS) 140-1, for cryptographic modules utilized within DoD PKI. Currently only Netscape is FIPS 140-1 certified. Microsoft claims it will be compliant with Windows 2000. This is an area of solid ground for the IT manager to stand on.

The choice of the correct hardware is an important decision for the IT manager. The decision centers on which type of disk arrays or mainframes will provide the most stability now and into the future [Ref. 8].

The choice of trustworthy software is another area of concern for the IT manager. Currently, DoD requires that contractors utilize the Trusted Software Development Methodology (TSDM) for software development. As with FIPS 140-1, DoD has chosen a mature standard to hang its hat on. However, there is a counter argument for the IT manager to consider. TSDM takes roughly 12 – 18 months to create an end product, but new Internet products are developed every 6 – 9 months. This disparity between software development and Internet product development could cause some problems for DoD [Ref. 8]. The IT manager must weigh the pros and cons of this problem. On the one hand TSDM produces a stable usable product. On the other hand, few companies can currently produce software-using TSDM. And when a company utilizes TSDM they

lose the agility to react to technology evolutions in the market place and are unable to deliver quick prototypes that seem to be so valuable today [Ref. 8]. TSDM causes the developer to be late, by several evolutions, with the technology in the market place. The IT manager has to determine, based on his needs, which avenue to go follow.

As discussed above, trustworthy people are a necessity for a PKI to function properly. They are currently the weakest link in the security chain. To ensure trustworthy personnel, a thorough screening process must be undertaken and violators must be punished with severity. Background checks, screening, echeloning levels of trust, and checks and balances should all be employed to ensure personnel trustworthiness. Personnel can be a huge time sink for the IT manager.

Policies and practices relates to the SOPs or guidance that personnel follow in the operation of the system. A lot of the guidance is found in the PKI's Certificate Policy (CP) and Certification Practice Statement (CPS). DoD already has a CP and CPS for its PKI [Refs. 9 and 10]. The CP and CPS are crucial element to the smooth operation of a PKI and a lot of detail and work must be put in to ensure their accuracy and thoroughness. A management hierarchy must be established to ensure there are checks and balances in place during the creation, review, and updating of these documents. The DoD has a strong foundation here.

3. Certification and Accreditation

Standards are the name of the game when it comes to certification and accreditation. Currently there are several standards organizations with significant power in the PKI arena: the Internet Engineering Task Force (IETF), International Organization for Standards (ISO), and the International Electrotechnical Commission (IEC). The last

two, ISO and IEC created the X.509 certificate format standard mentioned earlier. As a side note, RSA, which is a privately owned company, has published some very influential specifications; they are known as the Public Key Cryptography Standards (PKCS). In addition to standards bodies there are other organizations involved with creating policy, for instance the Public Key Infrastructure Working Group (PKIX), National Institute of Science and Technology (NIST), and the Federal PKI Steering Committee (FPKI). How is an IT manager to make sense out of this alphabet soup? A fair question and not one easily answered if you listen to industry. DoD is making efforts to provide input to these organizations so that the special needs of DoD can be incorporated in to any internationally recognized standard. This issue can not be stressed enough. If DoD goes down the Beta instead of the VHS standard's road it could cost DoD time, money, and interoperability. In addition, this is another area where the uniformed service members are not well served. It takes a long time to understand the alphabet soup outlined above, and service members just do not stay in any job long enough to be true players in this arena. The author feels a concerted effort on the part of DoD is essential, but DoD will have to leave the real work to our experienced GS and SES employees.

4. Warranty and Liability Protection

Warranty and liability protection deals with the legal consequences of administering a PKI. This is a huge area and is probably appropriate as a thesis topic all by itself. With that said, industry has been very keen to provide certain warranty and liability protection to its clients. Depending on the type of certificate issued, the degree of confidence in identity verification, different amounts of monetary protection are provided. DoD can not and does not do this. They do state what the warranties are in the

CP and CPS, but when it comes to negligent behavior they assume no financial obligation. Is this a big issue for the IT manager? The answer to this question is probably not. However, it is one he should understand considering his work environment.

C. AVAILABLITY AND SCALEABILITY

This portion of PKI management deals with the PKI's ability to expand and maintain continuous operations. The major areas covered are system back up and recovery, business resumption planning, customer response times, and binding service level agreements.

1. System Back Up and Recovery

System back up and recovery deals with a myriad of topics, which include data, equipment, telephone and network connectivity, power, and people. The amount of effort the IT manager focuses on these areas is related to the amount of fault tolerance he requires in his system. Data is the key element we are trying to protect with a PKI. Therefore, the ability of an enemy to deny us access to our own information is a big concern. The data in a PKI that must be secured, yet always made available, are directories of public and escrowed keys.

Key escrow is the storing of a copy of the encryption certificate's private key in a repository. This repository can only be accessed for official, approved business in cases of the subscriber's death or national security. Most organizations split the key so it takes two or more people to be able to access the private key. The important point is that this information must be stored in a secure facility and the information needs to be backed up at another site. Key escrow is a highly political issue that DoD PKI has mandated.

However, this is probably not a big in-house problem for DoD. Having said this, not all of industry supports key escrow. However, it is vitally important that information that is encrypted be able to be decrypted in times of national crisis. The key to key escrow is directories.

Directories for public keys are at the center of PKI management. This service is one of the power enablers in a PKI. The system needs to be to able support a person, router, or server, anywhere in the world, accessing another person's public key, at any time of the day or night. What then needs to happen? The end state would consist of mirror image redundant directories at all the CAs, which loads and deletes public keys automatically when certificates are created and expire. If an IT manager can make this happen, then he has truly earned his pay.

The other big use of directories comes in the form of key escrow. This is currently a big problem for DoD PKI. At the present there does not exist a central repository for all encryption certificate private keys. Right now units are manually storing these back up keys on site. This is a huge administrative burden and a logistical nightmare. What if Bob is transferred from San Diego to Norfolk? Do you cancel and then reissue the encryption certificate? What about all the old material he has encrypted? What about that material that is associated with a particular billet? Does each person have to have two encryption certificates one for personal use and one for the billet? Do you give him the back up for transport to the next LRA? Not a good idea unless you can prove he did not forge the back up copy. Do you mail it to Norfolk? What then needs to happen? The directories located at the CAs or RITSCs, RITSCS will be explained in Chapter IV, need to automatically store encryption certificate private keys during

encryption key generation. Their access should require two persons and the procedures should be clearly defined in the CP or CPS.

There are a lot of problems with directories and it all centers on the immaturity of the technology. Industry is struggling with these issues as well. Standards are coming together, but there is a lot of work yet to be done. If DoD wants PKI to be accepted and used by every uniformed and civilian member of DoD they must focus their attentions on directories.

The above discussion on directories and key escrow showed the significance of fault tolerant and redundant systems with data. The argument holds true with equipment as well. There must exist enough back up systems to meet an IT manager's threshold for fault tolerance. Earlier in the chapter, back up for power and ISPs were discussed. Again, the same argument holds true. The IT manager must determine his fault tolerance threshold and then work system and network redundancy to support it. People, however, were only discussed through the aspect of trustworthiness. The idea of trust can be expanded one step further. The degree to which an IT manger performs background checks, interviews, and installs internal control mechanisms is dictated by his fault tolerance threshold.

2. Business Resumption Planning

One issue that the DoD needs more work in is business resumption planning. It needs to clearly state what will happen when a system goes down and what procedures will be followed. They have begun this process, but more work is yet to be done. Industry has become very adept at this planning and DoD might learn some lessons from the work they have already done in this area [Ref. 8]. It should be clarified again, that

PKI is largely an immature technology and a lot of people are doing a lot of learning every day. There are no overnight fixes here. And if DoD and the Navy want its members to buy in to PKI they must move slowly and plan carefully lest they lose the confidence of the populace.

3. Response Times

Another issue for the IT manager is that of customer response times. Specifically, PKI transaction processing times and customer support times. If DoD truly wants PKI to be a success it needs to ensure that PKI transactions are processed rapidly. That is, people will not sit by aimlessly and wait minutes for an application to encrypt an e-mail or for days for the CA to issue a certificate. Enough bandwidth and throughput must exist for the system to work smoothly. The difference with PKI and other systems is that PKI is not something people perceive needing. Most people do not have a perceived need for security or infrastructure issues. They do perceive needing a word processor. The difference being that people will spend the physical and mental energies to work with the word processor, but they will not with a PKI system. It is so important for IT managers to deploy systems and applications that require very little on the part of the users to leverage the power of PKI.

In the past, DoD has not been known for its customer service. Consequently, members of DoD are a little dulled to the concept and for some it is a real heartache. To add to the possibility that PKI will be a success in DoD, they must create a paradigm shift with customer service. DoD needs to deploy a fully functional and "responsive" customer support system. People want to talk to people. Of course this costs money, but it should pay off big in the long run. Responsive means they need to be there at all times,

24X7. They should operate at this tempo until there is DoD wide buy in to the significance of DoD PKI. When this is accomplished, the knowledge base should be significant enough to scale back operations. If early on, people try to contact customer service and either can not get through, are put on hold forever, or are given misinformation, then the reputation of the customer service facility will be shot and DoD PKI's image will be tarnished. The results will be another classic example of a poor deployment strategy.

4. Binding Service Level Agreements

Binding service level agreements state what the quality of service will be at what instance in time. They also state in the advent of an outage due to "x" that business will resume in "x" amount of hours. Industry gives these quotes to their customers in order to "guarantee" their service. This could prove to be a good idea for DoD as well. This is especially true when DoD starts cross certifying its CAs with industry, federal government, and NATO. In fact, it may become a requirement. However, if DoD gets into the process now of evaluating its performance and providing guarantees of its service to its subscribers, then confidence will build in the PKI. People will learn to trust the system and so will industry. If confidence in the system is grown from within and not mandated, the system has a much better chance of succeeding. The IT manager might need to wait on this issue until the infrastructure is a bit more mature, but he should start thinking about the idea now.

D. CUSTOMER SERVICE SUPPORT

As mentioned earlier customer service and support is not one of DoD's strong points. It is essential to DoD PKI that it changes that paradigm. Customer service and support is centered on skilled personnel, a knowledge database, and answers to queries.

1. Skilled Personnel

The key element to providing good customer support is people. These people must be bright, motivated, and willing to learn. This roughly describes the average enlisted service member. Once the foundation is established, training must occur. This training must focus on security, PKI, applications, and solutions [Ref. 8]. The training is intense, but the concepts are not difficult to grasp. There just happens to be a lot of information and it takes time to learn, understand, and apply the knowledge. One doesn't finish a class on PKI on Friday and then configure the directories for a PKI on Monday. There is a lot of hands-on training and the service members seem to really enjoy the work. This is probably for two reasons: (1) it is leading edge technology and (2) they know they can use the information post service commitment. It is the second reason that is causing DoD and the Navy so many problems. It is very difficult to get first term service members to reenlist, for the same wage rate, once they have been trained. Some people just give the service members the basics and entice them to reenlist with promises of more advanced training. This works for some, but what about the CO of a ship who only has a small IT staff and needs all staff members fully trained now. This is a big problem for the IT manager. Two solutions are contractors and outsourcing. Both have merit, but neither is fully tactical. Some will say they will deploy, but during times of actual conflict, what is DoD's liability? DoD is caught in a "catch 22." They are damned

if they train the service members, who are tactical and can be fully deployed. And they are damned if they use contractors or outsourcing, where they are not tactical or fully deployable. The answer is a mix, but it is a very delicate problem that will exist for some time to come if the services do not address wages, benefits, or career paths for its IT service members. Having said all of this, lets explore knowledge databases and clear things up with an example.

2. Knowledge Database

Once the skilled personnel have been sourced and trained it is now time to develop a "knowledge database." A knowledge database is partly physical, but mostly mental. It is physical in that one must try to document everything that is learned, so that others may use the knowledge in the future. This often takes the form of turn over folders or SOPs, but in reference to customer support it entails some sort of decision support system (DSS) linked to a physical database. This is used to help customer service agents answer the questions and queries of the subscribers. This process takes a lot of time and know how on the part of the IT manager and his staff. Luckily there are some software applications already on the market that can help with this process. However, they do not address the mental part of knowledge databases.

The mental part is that part of learning people know, but can not really explain. For example, how someone knew to reboot the system instead of reinstalling the software. Everyone learns a little differently and therefore they come to conclusions and solutions differently as well. This is the mental part of the knowledge database that is vitally important to organizations today. To illustrate lets use Verisign as an example. They have 350 plus full time professionals working on PKI eight plus hours a day. Are

there 350 plus people in all the services that know what PKI is, much less it is there primary job [Ref. 8]? Yes, is probably the answer to the first half of the question, but no is the answer to the other half. Knowledge about PKI is growing every day, but DoD has a long way to come. The author thinks it is unrealistic to think that DoD can match mental wits with industry. With that said, customer support and service, at least from the help desk perspective, leans itself to outsourcing or contractors.

3. Answers to Queries

The last facet of customer service and support is focused on getting the answers to queries. This is really the mission of a help desk or a customer support group. It takes all of the above people, training, tools, and a knowledge database to answer questions. How do you know the questions are being answered correctly? The business answer is quality control, but it is really more than that. It is an IT manager organizing a customer support "team", team being the important word, drafting an implementation plan and support procedures, and supervising the result. There is a lot of work to be done here. DoD has only begun to address the customer support and service issue at the DoD PKI level. What are the services and their subordinate commands going to do?

This chapter addressed the PKI management issues that await the IT manager as he wrestles with DoD PKI. The management issues focused on the technology, policies, procedures, and practices, and operations of PKI. PKI is a complex and immature technology in some ways and a mature one in others. The author feels that DoD is heading down the correct information assurance (IA) path with regard to PKI, but that there needs to be a stronger emphasis on PKI management. And what resource drives almost all management decisions? Money is the answer. It is going to take a lot of

money to implement a DoD PKI solution that can address the issues presented in this chapter. And in this time of fiscally constrained resources, shrinking service populations, and high operational tempo; is DoD taking on too much. This author feels the answer may well be yes. The solution may take a paradigm shift in the way we think. The current paradigm consists of DoD doing a requirement's analysis and then submitting a request for bids. Companies then figure out how they can meet DoD's requirements; perhaps they can modify their systems, maybe just slightly, or maybe they have to write code form scratch. This author suggests a different approach. Instead of starting with a requirements analysis lets go see the vendors off the shelf products, learn their capabilities, and then go back and change our business processes to fit within the ready to use COTS solution.

IV. PKI IMPLEMENTATION STRATEGIES

Chapter II provided the reader with background information on public and private key cryptography and how a PKI works. Chapter III provided the reader with some of the management considerations that must be addressed when standing up or operating a PKI. Chapter IV will build on these foundation concepts and provide the reader with some implementation strategies the Navy could use in order to implement DoD PKI. Specifically, Chapter IV will answer the first two research questions outlined in Chapter I.

- How should the Navy organize its public key infrastructure in order to most efficiently and cost effectively implement DoD PKI?
- How will the Navy distribute key pairs to 365,108 active duty, 196,986 ready reserve, and 195,058 civilian personnel [Ref. 5]?

Before these two questions are answered, the author will provide a summary of the Navy's "tentative" plan to implement DoD PKI. The author says tentative, because the Navy's plan has not been finalized. There are numerous discussions under way with regards to architecture, funding, and implementation strategies. All of these issues will be addressed to some degree in this chapter.

A. THE NAVY PLAN

As stated above, the Navy's current implementation strategy is yet to be fully defined. The author will outline the Navy's "current" plan in reference to the two primary research questions. The first question asks how the Navy will organize its public key infrastructure in order to implement DoD PKI. Figure 4-1 shows the DoD and Navy public key infrastructure.

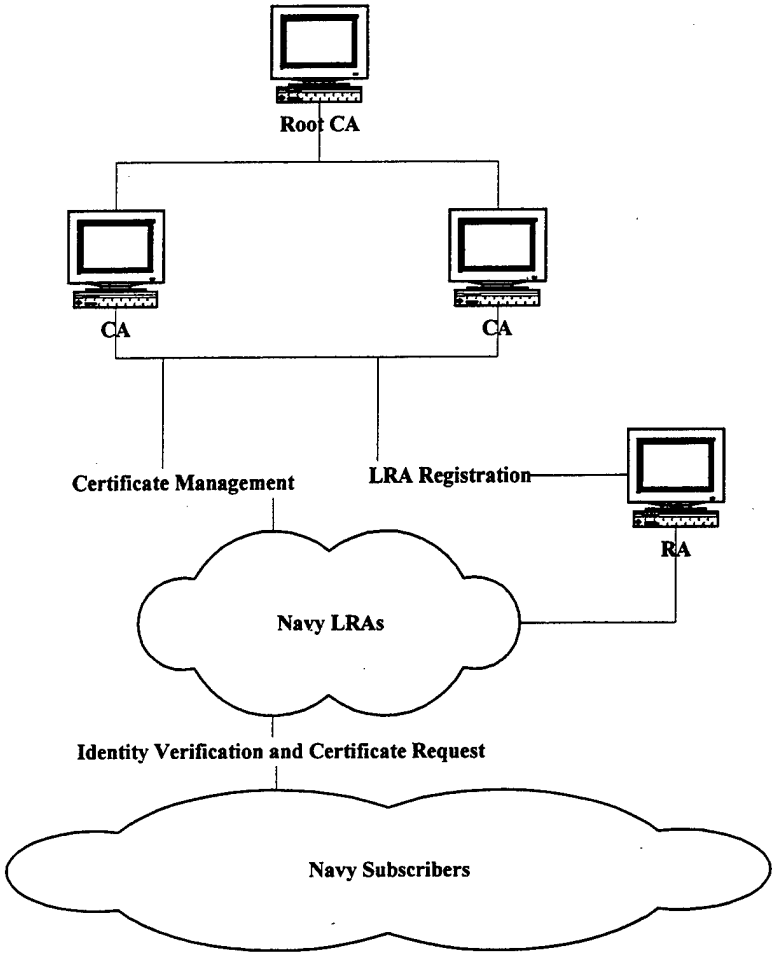


Figure 4-1. DoD and Navy PKI

The Navy intends to establish one RA at Director Communications Security Material System (DCMS). The RA will be responsible for authorizing LRAs, administering the Navy's CRL, and communicating with the DoD PKI CAs. The Navy has left the determination of LRA distribution up to its 34 second echelon commands; these commands are outlined in the Navy's Standard Navy Distribution List (SNDL). Each of the second echelon commands is free to organize centrally or de-centrally its LRAs based on mission, need, etc. This will most likely lead to a heterogeneous distribution and organization of LRAs throughout the second echelon commands. The

second question asks how the Navy will distribute key pairs to all its members. The "current" Navy plan does not address this question. The reader of their plan can only assume that each second echelon command will be responsible for devising and implementing its own key distribution system. Again, no thought is given to creating a homogeneous plan throughout the entire Navy. From the above it becomes pretty clear that the Navy does not plan to centrally control the implementation of DoD PKI and that their plan is still very immature. As time goes by, a lot more detail will be promulgated and the "current" plan may change completely.

B. DOD PKI TIMELINE

Before the author addresses different implementation strategies in reference to the two basic research questions, one important issue must be clarified – time. The Navy's implementation of DoD PKI is constrained by a fairly aggressive DoD PKI implementation time line. This time line was promulgated by the Under Secretary of Defense (USD) in his memorandum of 6 May 99 [Ref. 11]. The important dates are:

- By June 2000, all category 1 mission critical systems operating over unencrypted networks and employing public key technology must fully implement Class 4 certificates and tokens [Ref. 11].
- By June 2000, all Navy, not publicly accessible web servers will at a minimum have a Class 3 server certificate [Ref. 11].
- By October 2000, all Navy second echelon commands must have the infrastructure required to issue Class 3 certificates to all members of its command [Ref. 11].

- By October 2001, all Navy personnel, both civilian and military will have been issued a Class 3 certificate [Ref. 11].
- By October 2001, all Navy and Navy-interest not publicly accessible web severs will require client identification and authentication with, at a minimum, Class 3 certificates [Ref. 11].
- By October 2001, all electronic mail sent within DoD must be digitally signed [Ref. 11].
- By January 2002, all Class 3 certificates will begin to migrate toward Class 4 certificates. All new certificates will be Class 4 certificates [Ref. 11].
- By December 31, 2002, all category 2 and 3 mission critical systems operating over unencrypted networks and employing public key technology must fully implement Class 4 certificates and tokens [Ref. 11].
- By December 31, 2002, all Navy personnel, both civilian and military, will have been issued a Class 4 certificate [Ref. 11].

As can be easily seen form the bullets above, the DoD PKI implementation timeline is very aggressive and convoluted. The timeline is scheduled for review January 2000 [Ref. 11]. This author predicts some date adjustments will follow as a result of funding and technology development issues. These ideas will be clarified later in the chapter.

C. NAVY ARCHITECTURE

The Navy's PKI architecture in support of DoD PKI needs some adjustment. Currently, the plan calls for one RA and multiple LRAs. The number of LRAs could grow to 1,800 or more, depending on second echelon LRA deployment strategies. The

author will now provide some alternate architectures and outline their respective advantages and disadvantages.

1. Navy Marine Corps Intranet (NMCI)

The concepts surrounding the Navy Marine Corps Intranet (NMCI) are still in the foundation stages. It is believed that NMCI will be a more robust version of the Navy Wide Intranet (NWI). However, due to lack of material currently available surrounding NMCI, the basic architecture supporting the Navy Wide Intranet (NWI), see Figure 4-2, will be used to illustrate how the Navy could implement DoD PKI.

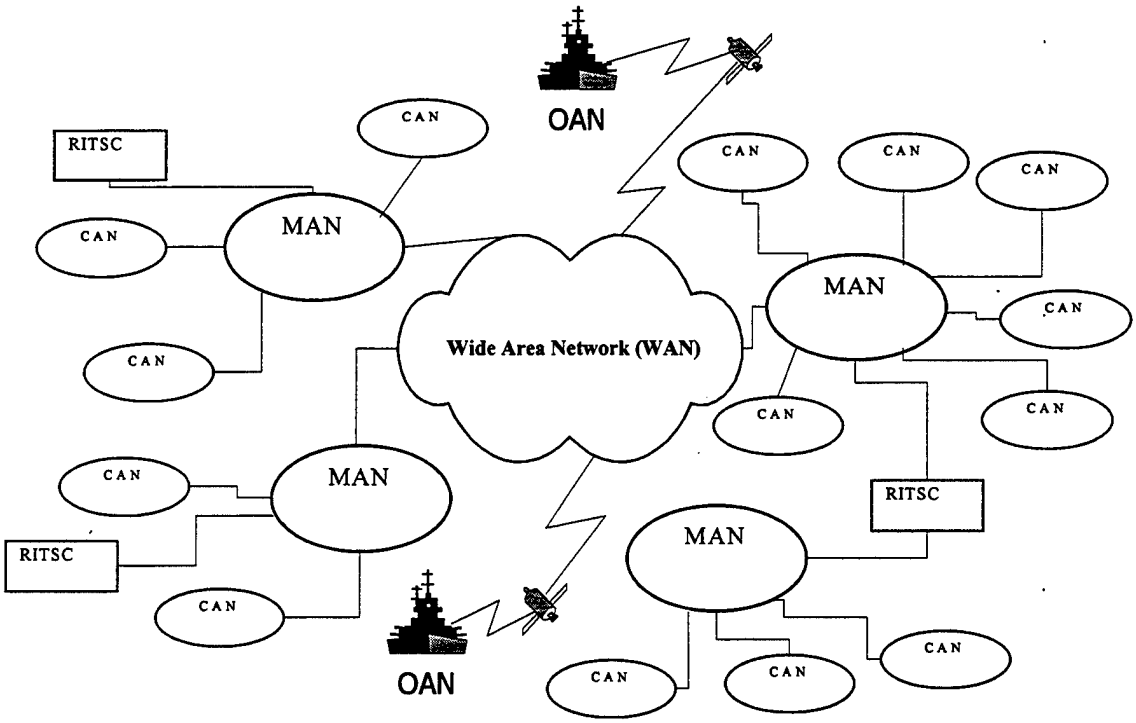


Figure 4-2. Navy Wide Intranet (NWI)

The basic components of NWI are:

a. Wide Area Network (WAN)

The Wide Area Network (WAN) or Department of the Navy (DON) Enterprise Network provides connectivity for all Navy and Marine Corps' Metropolitan

Area Networks (MANs). There are multiple varieties of WANs, i.e. NIPRNET, SIPRNET, etc. [Ref. 12]. The WAN connects to the Internet via switch or router.

b. Metropolitan Area Network (MAN)

The Metropolitan Area Network (MAN) provides connectivity for Navy and Marine Corps' Bases, Posts, Camps, and Stations with their Regional Information Technology Service Center (RITSC) and the WAN. The MAN does not have direct access to the Internet. It connects via switch or router to the WAN [Ref. 12].

c. Campus Area Network (CAN)

The Campus Area Network (CAN) provides connectivity for Navy and Marine Corps' tactical and support units. The CAN does not have direct access to the Internet. It connects via switch or router to the MAN. The only exception is for a geographically disparate CAN; it utilizes VPN and connects to a MAN or RITSC [Ref. 12].

d. Operational Area Network (OAN)

The Operational Area Network (OAN) provides connectivity for operational forces. The Operational Area Network connects to a CAN or WAN through satellite or radio frequency (RF) transmissions. It does not directly connect to the Internet. It connects to the Internet through one of the structures outlined above.

e. Regional Information Technology Service Center (RITSC)

The Regional Information Technology Service Center (RITSC) is operated by Navy and Marine Corps personnel and provides network services to one or more MANs [Ref. 12]. There exists the potential to outsource all services performed by the RITSC.

2. Regionalization

NWI provides a sound architecture for the Navy and Marine Corps' networking needs to follow. PKI is a highly network intensive operation. All of the following PKI management activities are well suited to a networked environment:

- Key Escrow
- Key Recovery
- Public Key Directory Services
- Certificate Revocation List Management
- Key Generation
- Certification Issuance
- Identity Verification
- Secure Communication
- Customer Service

Therefore, it is the author's proposal to collocate these activities at the RITSCs. The current NWI plan calls for 9 –12 RITSCs. These RITSCs would be the Navy's only connection to the WAN. Therefore, like the Marine Corps Enterprise Network (MCEN), the Navy's WAN could become self-contained. By doing this they would significantly increase their information security by reducing the number of pipes entering the Navy's network architecture. Currently, there are countless pipes extending into the WAN. It is very difficult to control and manage such a network. And currently, little management is taking place within the network. If the Navy regionalizes its control over its networks it gives itself the ability to centrally manage all of its subordinate networks, i.e. MANs,

CANs, and OANs. It also gives the Navy the ability to centrally control all of the services that utilize the network, i.e. PKI and Navy White Pages. The RITSC is the ideal location for the customer service help desk too.

The author further proposes that the RITSCs become sub-CAs to the two primary CAs in Chambersburg, PA and Denver, CO. These CAs would have the collateral job of being RAs too. The idea is to reduce the time required to perform certain PKI functions, i.e., key generation, key recovery, key escrow, etc., and limit the requirement for information to cross the WAN until off peak hours. By allowing the sub-CAs located at the RITSCs to issue certificates, they would have this authority because their public key was signed by one of the DoD CA's private keys; there is a reduced requirement for information to pass outside of the region. The obvious exception to this would be the process of creating mirror images of the public key and CRL directories. This could occur during non-peak hours though. Regionalization gives the Navy's network some robustness. By reducing cross network communications to those absolutely necessary, one can free up bandwidth for those applications that truly need inter-region communications, i.e. C^2 or flash intelligence updates.

One more variant to the paragraph above is to outsource the two DoD CAs as well. The issues here are the contractors ability to handle the extremely large volume of certificates, will be over 2,000,000 and no industry vendor has ever deployed a PKI of this magnitude, and their ability to meet DoD PKI's requirements as outlined in the DoD CP and CPS. The biggest sticking point for vendors is in person ID verification. However, this will not affect their ability to run the DoD CAs, just the LRAs. A solution

to this problem will be provided later in the chapter. It appears the DoD CAs are a good candidate for outsourcing.

Regionalization also gives the Navy the opportunity to leverage the power of a consolidated help desk. Each region will have its own idiosyncrasies. And by having one centralized source for questions about the system or services that flow over the system, customer service representatives can become intimately in tune with their region. They can truly learn what the customer needs and be better prepared to answer those needs. In addition, by collocating PKI services within the RITSCs the Navy can have one help desk per region versus one per system. This also gives the RITSC staff the ability to cross train and become familiar with multiple systems and services. This becomes very convenient, because all of the hardware is located under "one" roof.

RITSCs also ease training. This is because the RITSCs could become the centralized training facility for their region. Each RITSC could set up classrooms for lectures and then proceed to give the students hands on training with the equipment. This type of real world practical application is invaluable in today's fast pace environment where knowledge needs to be accessed rapidly. In addition, travelling trainers and contractors would have facilities to regularly visit and could provide a series of lectured programs.

Because NMCI is going to join the networks of the Navy and Marine Corps together, this regional concept will make Navy and Marine Corps personnel work together more closely and enhance the atmosphere of a Navy/Marine Corps team. The RITSC concept will also create a career path for Navy and Marine Corps information technology personnel. Sailors and Marines would rotate sea or fleet service tours with

shore or base service tours. Junior Sailors might start off working on smaller ships and CANs and then as their knowledge grows move up to MANs or RITSCs and carriers.

Regionalization gives the entire network redundancy in its services and its architecture. If one RITSC goes down, then a user's request for a public key or the current CRL will automatically be forwarded to the next closest RITSC. Again, this is possible because of mirror directories located at the RITSCs.

NWI or soon-to-be NMCI is a powerful concept and the organization and security it provides the Navy/Marine Corps team should be leveraged to benefit the Navy's implementation of DoD PKI. NMCI organizes the Navy's architecture for DoD PKI, but it still puts a large burden on the operating forces, mainly in the arena of personnel costs. To answer this problem the Navy must match the architecture of NMCI with the concept of biometrics.

3. Biometrics

One of the big costs for implementing DoD PKI is personnel. Specifically, the personnel required to operate the LRAs. The active duty forces are already strained to meet their operational and training commitments. Pulling more personnel away form them does seem like a good idea. The author proposes leveraging the power of biometrics and the Defense Enrollment Eligibility Reporting System (DEERS) and the Real-Time Automated Personnel Identification System (RAPIDS) to counter this personnel requirement. DEERS and RADIDS are a collection of independent, but closely coupled systems, which contain personal information on every past and present service member and civilian employee [Ref. 13]. Part of an individual's record is the biometric minutia of a fingerprint. RAPIDS' personnel collect these biometric minutias when a

uniformed service members apply for original or updated identification (ID) cards. How then does biometrics help the LRA personnel problem? The answer lies with ID verification.

The current DoD policy requires in person verification of identity before a DoD identity certificate can be issued [Ref. 6]. The author suggests that this does not do what it says it does and offers biometrics as a viable alternative. First, when an LRA verifies someone's identity they are doing so solely based upon the credentials presented. Currently, these credentials consist of a DoD ID card. All the LRA does is physically sight the card. Is the process of physically sighting a DoD ID card sufficient for proof of identity? The author suggests not. DEERS/RAPIDS personnel issue DoD ID cards after presentation of an original or notarized copy of a birth certificate, marriage license, and social security card. If a person provides false credentials to the DEERS/RAPIDS system and they are not detected, there will be no way to officially refute their identity. This is because their actual biometrics will forever be linked to their false birth certificate, marriage license, and or social security card information. The belief is that there are sufficient checks and balances in the DEERS/RAPIDS registration process to catch any such false documents. However, what about the individual who has a fraudulent DoD ID card? This could be handled with the current registration process if LRAs used a bar code reader to read the picture and other personal information contained on the card's bar code. This does not help with the personnel problems and in fact worsens their situation with increased procedures per certificate subscriber.

How do you ensure identity and reduce the second echelon command's of the burden of LRAs? The answer is to automate the whole identity verification, certificate

request, and certificate issuance process. Naysayers would declare that LRAs are what ensures the integrity of the system. The author proposes that the LRAs, because they are human and fallible, are the weakest link in the security chain. The author proposes three ways this system could work.[1]

a. Proposal One

The first proposal centers on a stand-alone computer with the following properties:

- Connected to the DON Enterprise Network
- Ability to connect to the Internet
- Finger print scanner
- Smart card reader
- Connection to a printer

Once the system is secured, procedures must be followed. A step by step example, see Figure 4-3, will best illustrate Proposal One.

First, the DoD uniformed service member or civilian employee gets a DoD smart card from an issuing source, this might be the unit Communication Security Materials System (CMS) custodian, administrative personnel, or a DEERS/RAPIDS center.[1] Next, the user sits in front of a computer with the above properties. He then opens up the certificate registration application. He fills out the application form with his name, SSN, birth date, etc. Once this is done the subscriber initializes the smart card. Part of this process requires the subscriber to place his finger on the finger print scanner.[2]

[1] As a note, the hope is that the DoD smart card will be the DoD ID card. This idea will be expanded later in the chapter.
[2] In the rare scenario that an individual could not utilize a finger print scanner, for whatever reason, a retinal scanner could be used.

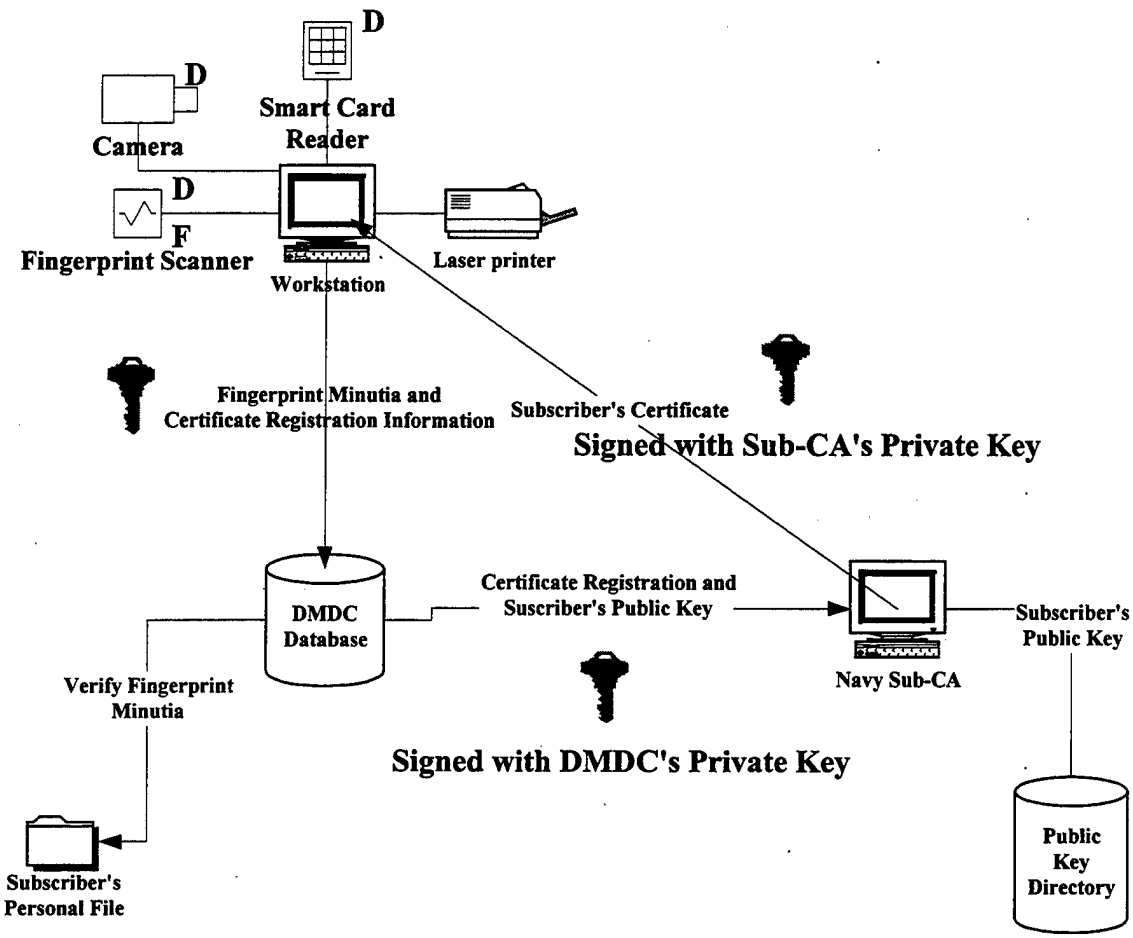


Figure 4-3. Proposal One

The scanner takes an image of the fingerprint and converts it into minutia. This minutia is then loaded to the smart card. This will forever be the user's method of authenticating himself to his smart card. To ensure it got a clean read the user would remove the smart card, replace it, and try to activate it by placing his finger on the finger print scanner. If all of this is successful, the next part of the process begins. If not, the process begins

again by clearing the smart card and starting over or contacting the online web tutorial or help desk for assistance.

The next part begins by having the user generate an identity key pair on the DoD smart card. Once the key pair is generated, the public key is attached to the certificate request. Once this is done, the registration application initiates a VPN connection to the Defense Manpower Data Center (DMDC) to verify the user's identity. Using the information the user input into the registration application, the person's biometrics information is pulled up. The biometrics stored at DMDC and those taken at the terminal are compared. If they match and all the information entered in the application is correct, the certificate request is signed with DMDC's private key. DMDC then initiates a VPN with the author's proposed model of a Navy sub-CA. The sub-CA verifies DMDC's certificate with DMDC's public key and then issues the certificate directly to the user at the terminal. The registration application on the computer then stores the certificate on the DoD smart card. At the same time, the public key directory at the RITSC is being populated with the new user's public key by the sub-CA, collocated at the same facility. The last step is for the user to remove his smart card and the process is complete. There is no requirement for an LRA to verify the subscriber's identity, to input information into the certificate request, or to manually escrow keys. The LRAs will be busy enough managing the certificates of the command's hardware. In addition, the LRA will be responsible for answering questions of those users who are too obstinate to use online help, tutorials, or the RITSC's help desk.

b. Proposal Two

Proposal two, see Figure 4-4, is similar in design to proposal one except the concept of something you know is added. Verification of identity is strongest if you authenticate for these three principles:

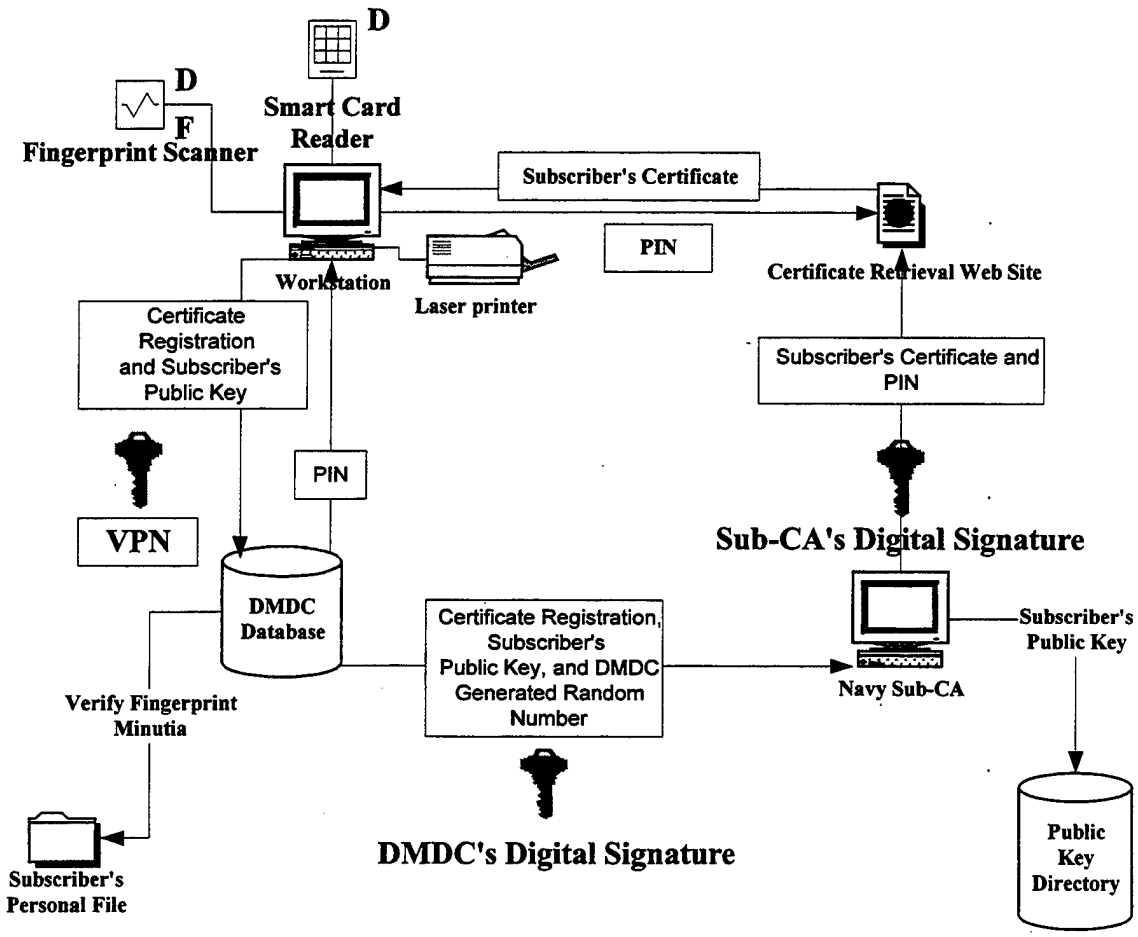


Figure 4-4. Proposal Two

- Something you are (the biometrics of your finger print)
- Something you have (a smart card, preferably one that doubles as your ID card)
- Something you know (personal identification number (PIN))

In proposal two, after DMDC verifies your identity it generates a random number, attaches it to your certificate request, digitally signs the request, forwards the request to the sub-CA, and then automatically prints off the number on the subscriber's directly connected printer. While still sitting at the terminal the subscriber is told where to go on the Internet to get his certificate. The subscriber closes the certificate request application and then enters the web site where he was told to pick up his certificate. The web site asks the users to authenticate himself with something he knows, in this case the one time PIN. In this proposal, all three methods of identity verification were employed, but some additional procedures were added as well. The author feels the system provides a greater degree of security, but that the overhead with the additional procedures, especially the printer, might be too high.

c. Proposal Three

Proposal three has as its basic assumption that DoD will leverage the current organization of DEERS/RAPIDS workstations worldwide to address the requirement for in person identity verification. Currently there are 1,318 workstations at 878 sites in 13 countries [Ref. 13]. This infrastructure could be used with DoD's current PKI processes for certificate request and in-person credential verification. In addition, the added security of biometrics comparison could be easily accomplished. The problems would be with staffing and funding. The number of workstations would have

to be increased and additional civilian personnel hired, but the infrastructure is already in place and could be leveraged almost immediately. The benefit of this idea is that the new hires could be cross-trained in DEERS/RAPIDS procedures and DMDC as a whole would benefit from a larger, more diverse skill set.

Proposals one and two could be used with two variants of proposal three. In the first, the DEERS/RAPIDS personnel could physically sight the credential of the subscriber and then reference him to a kiosk where he could follow the procedures of proposal one or two. The verification of credentials could be enhanced through scanning of the DoD ID card through a bar code reader. This process is already available at the workstations. The other variant of proposal three is that the subscribers could just show up and utilize kiosks set up at the DEERS/RAPIDS centers. The subscribers would be free to utilize either proposal one or two; whatever was the current procedure. The DEERS/RAPIDS personnel would be there to address their DoD ID card needs, very handy if the DoD smart card turns out to be the DoD ID card, and act as an immediate help desk in the event of problems. The last idea has a lot of robustness and flexibility in it. Some quantitative studies on queuing theory and marginal cost should be run to determine the best fit, but utilizing an in place infrastructure with enhanced security has to be looked at hard.

As an ending note, proposal one and two could easily be done at any location. With this the author means somewhere other than a DEERS/RAPIDS station or a unit LRA workstation. Proposals one and two can be done anywhere the hardware and connectivity requirements addressed above are met. The key with any of these proposals is to remove the burden from the uniformed services and service members. There will be

plenty of work for LRAs to do just keeping up a command's hardware certificate needs. This is especially true since the current DoD PKI policy only addresses certificates for servers, but intends to expand that to routers, switches, repeaters, sensors, etc.

4. Smart Cards

Before moving on to the second primary research question, we need a discussion on smart cards. A smart card is a hardware token which is capable of storing a person's public and private keys. It is also possible to store additional information on the card like fingerprint biometrics, a PIN, etc. In addition, some smart cards can store a cryptographic module capable of generating public and private key pairs on the card. Smart cards are very versatile and DoD can utilize them in a variety of ways, i.e., weapons issuance, mess hall admittance, and medical and dental applications. There are some debates going on within industry as to how much information should be stored on a smart card [Ref. 14]. If the memory on a card is large enough you could store all of a service members medical, dental, and personnel records. Cards capable of carrying this much information tend to be quite expensive. A problem with storing this much information on the card is what happens when it falls into the wrong hands, i.e., the service member becomes a POW. Then the enemy would have access to a lot more information than just a service member's private key. DoD's plan for a smart card is moving in a different direction.

The DoD is looking for a standards based card capable of storing a small amount of data. This data would be used for authentication purposes. DoD's current plan is to leverage the power of PKI and the information security it provides. The idea is to put a FIPS 140-1 compliant cryptographic module on the card. This module would create the

subscriber's public and private key pair directly on the card. It would not be possible to remove the private key from the card. The public key would be exported from the card to appropriate directory systems. In addition to the key pair, a finger print reader would store a person's fingerprint minutia on the card too. This information would be the subscriber's authentication mechanism, before he could access the card. This idea is much more robust than PINs. PINs can be lost, but it is very unlikely some one's fingerprint will change.

Once the keys are located in the smart card, access control lists (ACLs) could be used to grant or deny people permission to facilities or services based on their smart card. For example, when a Sailor wanted to draw his weapon from the armory he would put his smart card in the reader and then activate it by putting his thumb on the fingerprint scanner. Then the armory application could verify the Sailors identity by signing a communication with the user's public key. The smart card could respond by opening the communication with the subscriber's private key, this is called authentication, and then responding back to the armory's application by digitally signing the response with the subscriber's private key, this is called non-repudiation. With this procedure the armory would positively know the identity of the person trying to draw the weapon and would have a digital signature to verify the person has the weapon out of the armory. This idea is easily extended to mess halls, medical and dental facilities, or building access. The only management issue is the management of the ACLs. This would have to be done by a person, but could be made painless with access to the public key directories, a well written application, and a nice graphical user interface (GUI).

What then is the problem with smart cards? The answer to this question is standards and price. As with directories and CRLs there is not an internationally accepted standard for smart cards. This is slowing their development and the DoD's commitment to a particular style, vendor, etc. The other issue is cost. Currently, the DoD PKI implementation plans calls for all DoD personnel to be issued a class 4 hardware token, i.e., smart card, by December 31, 2002. This means the Navy would need to purchase cards for 365,108 active duty, 196,986 ready reserve, and 195,058 civilian personnel [Ref. 5]. Smart cards will be quite an expensive venture for the Navy. This cost is expanded by the need for smart card readers as well. Ref. 15 puts the cost of smart cards and readers at $50 for the pair. This extends out to $37,857,600 for smart cards and readers for all Navy personnel. These numbers do not take into account the potentially large numbers of smart cards and readers required for all the Navy's current and future PKI enabled hardware. The figure above appears to be an even larger amount of money when one realizes that currently there are no funds in the POM in support of the Navy's implementation of DoD PKI [Ref. 15]. It appears the Navy is in a quandary. This may be true, but the answer to this question is located within the second primary research question.

D. KEY DISTRIBUTION

For DoD PKI to be a success in the Navy two issues must be address:

- Which type of key should be implemented?
- How are those keys going to be distributed to the Navy expeditiously and efficiently?

1. Key Type

The type of key issued will be of great importance to all involved. But before the author provides his recommendations, a quick review of DoD mandates is in order.

- By October 2001, all Navy personnel, both civilian and military will have been issued a Class 3 certificate [Ref. 11].
- By December 31, 2002, all Navy personnel, both civilian and military will have been issued a Class 4 certificate [Ref. 11].
- By December 31, 2002, all category 2 and 3 mission critical systems operating over unencrypted networks and employing public key technology must fully implement Class 4 certificates and tokens [Ref. 11].

The DoD has promulgated a very aggressive PKI implementation timeline. This timeline affects and overlooks many things. It does not account for the military's Planning, Programming, and Budgeting System (PPBS), the Program Objectives Memorandum (POM) cycle, or the acquisition life cycle of systems and products. Having said this, the Navy's back is against the wall with regards to the first deadline. In approximately 13 months they have to distribute class three certificates (on 3 1/2-inch floppy disks) to over 750,000 people. This is no easy task, especially since the infrastructure is nowhere near in place. To exacerbate the problem, 14 months after they finish issuing the class 3 certificates, they have to issue class 4 certificates, smart cards, to the same 750,000 people. The author thinks this is going to be just too hard and too painful for an organization like the Navy, especially when it has a reputation of not always following the CNO's directions explicitly. Therefore, the author proposes a strategy or plan of

delay, delay, and delay. The author feels the Navy is better served implementing an infrastructure and key distribution plan focused around smart cards. It will be a waste of time, energy, and monies to make the October 2001 deadline for class 3 certificates. The Navy's energies are better served crafting a well thought out plan for class 4-certificate deployment. The author feels the Navy should not blatantly disobey the orders of the DoD CIO and the USD. Instead, they should deploy class 3 certificates in support of their servers. They should also issue class 3 certificates to a "limited" population that has an immediate need for them, i.e., PKI pilot members, Flag Officers, etc. The Navy should enter into negotiations with the DoD CIO and USD. They should clearly brief their long term plan, show how the infrastructure will work, show a good faith effort at meeting the other deadlines, and demonstrate the benefits of waiting. They could illustrate the advantages of waiting with JUMPS. JUMPS is an example of a system that was fielded too early and it took a long time before the services got it right. The Navy's plan should be accomplished by outlining the advantages from a properly programmed and budgeted system. This being said, the author will now address why smart cards are the key of choice for the Navy.

For DoD PKI in the Navy to be a success, smart cards need to be employed. This is true for many reasons. The first is symbolic. A smart card is the same size as a driver's license or a military ID card. People are used to dealing with credit cards and ID cards. Therefore, they will be more inclined to use and embrace something they are more familiar with. This is important for PKI to take hold in the Navy. Secondly, it is simply a much more secure mechanism for storing the subscriber's private key than a 3 1/2-inch floppy disk. If the current DoD implementation plan progresses unchanged, by October

2001, the Navy will have over 750,000 computer disks with private keys. These keys are secured with a PIN. These PINs are easily forgotten or worse yet, written on the front of the disk. In addition, disks, because of their odd shape and non-symbolic form are often mistreated, lost, or easily copied. If the reader believes the hypothesis that the user is the weakest link in the security chain, it would stand to reason that a mass deployment of diskettes with private keys could be a tremendous problem. If all goes according to this thesis, the Navy will have a strong implementation plan based upon smart cards. How then is the Navy going to get these keys to all of its personnel?

2. Physical Key Distribution

Physical key distribution can be viewed from several perspectives. The first is from the present. In the Navy there have been very few keys issued. Therefore, the current perspective is how to distribute keys to all of the Navy's personnel. The other perspective is from the future. What does the Navy want the future to look like? How does the Navy want daily operations to progress? How will the Navy deliver services, i.e., pay, medical, training, etc., to its people? The last perspective is that of the transition form current to future. How does the Navy move form point "a", which is now to point "b" which is two to five years from now? Ref. 16 sees this process as having three distinct phases:

- Initial Deployment
- Ramp-up
- Sustainment

The author will address each of these phases and will chronologically move from sustainment to initial deployment, future to present

a. Sustainment

The author believes the future will be a more web based computer environment. Users will be mobile and will need to be able to plug-in and gain a connection to information form anywhere in the world and at anytime of the day or night. To support this, the Navy should decentralize PKI registration and certificate maintenance for the subscriber. To do this, the Navy needs to web base its PKI processes and provide functionality from any platform. This means all a user needs is the appropriate software, fingerprint scanner, a smart card scanner, and an Internet connection. The author believes that in two to five years the fingerprint scanner and smart card reader will be internal to the CPU and the Internet connection will be wireless. Based on this premise, users can access a sub-CA from anywhere in the world and renew, request, or revoke a certificate or whatever else he needs to do. Therefore, when someone joins a ship he or she can easily get additional certificates by sitting in front of any workstation with his smart card. However, if the DEERS/RAPIDS asset model is utilized, then increased hours of operation will be required, i.e., no longer will 8 a.m. - 5 p.m. be acceptable.

How will new service members and civilians initially get smart cards and certificates in the future? Once a service member completes their initial training, i.e., boot camp, OCS, ROTC, or Naval Academy they will be given access to a computer at their initial training school upon completion of training and prior to check-out. In this way all service members arrive to a fleet or shore command with a certificate in hand. For new civilian employees, the respective command's HRO will be responsible for having computers available so that after hiring, but before their first day of work they

have a certificate. The future seems manageable based on the plan outlined above, but how does the Navy get from its current state to the future state? The answer is ramp-up.

b. Ramp-up

There does not appear to be any "easy" way to distribute keys to over 750,000 personnel worldwide. There are two ways to view ramp-up. One is from the perspective of the current policy of in person ID verification and the other is though remote ID verification utilizing biometrics. In the first case, teams of LRA administrators must be gathered from all over the Navy and sent form command to command. These travelling "road shows" would set up in a huge common area, i.e., a gymnasium, and people would be sent in by command, preferably to get their certificate and smart card. This process could take care of most of the Navy, but there would be those inevitable stragglers that just can not be located or are unavailable when the road show arrives. The local LRA administrator would then be responsible for taking care of these people. These people's numbers could be quite large and the process would be quite time consuming. Therefore, this is not a great idea.

If the second process is employed, the problems outlined above could be avoided. There would be no need to gather LRA administrators from around the Navy to perform this travelling "road show." Instead the Navy could outsource the whole process. Teams of contractors could fall upon the Navy almost overnight. They would set up a layout similar to the one outlined in the gymnasium example above. However, the computers would be for the subscriber's use. The contractors would be duty experts in the process and would be able to assist users on the spot. This whole set up would be more user friendly and the author thinks more amenable to Navy personnel. All people

who missed the "road show" could simply use their existing computer; as long as it had the requirements outlined above, and get their certificate at their desk. The RITSC help desk would be available to answer questions when they arose. Both scenarios would have a tremendous logistics tail, but could be managed with proper planning. The second scenario has the added benefit of no Navy personnel being pulled away from their commands; the contractors would do all the work. In addition, the contractors could provide PKI training for all personnel before or after enrollment.

c. Initial Deployment

Initial deployment is fairly straightforward. LRA administrators have to be set up and trained for all of the hardware certificate installations. In any scenario this requirement still exists. They would also have the collateral responsibility of issuing software or hardware tokens to those individuals with an immediate need. These personnel should be scrutinized because of the requirements of manual, local key escrow, no means of key recovery, poor directory services, and a lack of money and personnel to deploy PKI at this time. The focus of initial deployment should truly be the hardware. If the Navy can get its routers, servers, firewalls, switches, etc. properly PKI enabled, then it has gone far in solidifying its IA wall of protection. During this phase a lot of personnel training will be conducted and a lot of things will be learned. It is a very important phase and should not be trivialized. What happens here sets the tone for Navy PKI in the years to come.

V. MANAGING CHANGE

A. THE CHALLENGE OF CHANGE

The purpose of this chapter is to address those change related issues surrounding the Navy's implementation of DoD PKI. There are many issues which arise when talking about change and how to manage it: forces that inhibit and create change; vision of what will be changed; how to implement the change; how people respond to change; and what it means to be a change agent [Ref. 17]. These issues answer four fundamental questions regarding managing change:

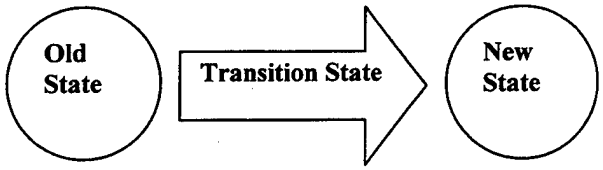
- What is to be changed?
- How is it to be done?
- Who is affected?
- What are the consequences so far? [Ref. 17]

This chapter will answer these questions and provide insight into areas the Navy should focus on in order to create the change necessitated by the introduction of a new information technology. It will also address how to ease the burden of change [Ref. 17]. Before the issues of managing change are addressed, this chapter will outline the forces that drive and enable change and what reactions change evoke. [Ref. 17]

1. Transitional Change

"Change is a planned or unplanned response to pressures and forces." [Ref. 17] The Navy's implementation of DoD PKI is just that. It is a response to the Under Secretary of Defense's (USD) call for all DoD computers and web sites to utilize public key cryptography at the sensitive but unclassified (SBU) and below level. The change the Navy and DoD are undertaking is a transitional change, see Figure 5-1. The end state, a fully operational PKI, is understood and so is the old state, which is our current

state. What the Navy and DoD are doing is trying to manage the interim transition state. [Ref. 17]



(No PKI) (PKI Implementation) (DoD PKI)

Figure 5-1. Transitional Change [From Ref. 17]

The Navy requires a transitional change because it is implementing a new technology, DoD PKI. This implementation will cause some reorganization and will involve several transition steps, i.e., pilots, phased in operations, and training [Ref. 17]. An important consideration once the type of change is identified is when to change.

2. Timing

When to initiate change is important. The culture and environment in the Navy may not be right for change now. However, as is usually the case in the armed forces, timing is not given much thought. The Under Secretary of Defense (USD) is being fairly forward thinking with his thoughts concerning the requirement for a DoD PKI. Not so much based upon PKI as an idea, because it has been around since 1989 with the Defense Messaging Service (DMS), but because of the scale of the proposal. He proposes that every DoD personnel, both military and civilian, be given a key pair. He is anticipating the need for secure e-mail and web site access as a critical security feature in the future. This is almost intuitive, once you learn that nearly 95% of what the DoD does operates over public networks [Ref. 4]. The Under Secretary of Defense (USD) wants all web sites PKI enabled by June 2000 and all e-mail encrypted by October 2001. The idea to

create a DoD PKI is not in response to a crisis, which would have the affect of rallying the troops around it, but in response to what he sees as a future requirement. If the proposed change is not in response to a perceived need by the masses, how then is the change going to be enabled so it will be effective? [Ref. 17]

3. Enabling Change

Enabling change to be effective deals with several strategic issues: pace, scope, depth, publicity, and supporting structures. [Ref. 17]

a. Pace

Pace deals with time and change and how they are related. The current environment in DoD does not dictate a rapid pace for implementation, but does dictate a steady pace. Many problems will arise if the Navy and DoD try to implement PKI prematurely. However, at the same time, the Navy can not wait to begin planning and implementation until they know all the answers, because if they did they would be in a totally reactionary mode. [Ref. 17]

b. Scope

The scope of the change deals with its breath. The DoD is starting small and then expanding its scope over time. It established the Root CA (at Finksburg, MD) and two sub-CAs (at Chambersburg, PA and Denver, CO) and is starting to use PKI with a pilot application, the Defense Travel System (DTS). [Ref. 17]

c. Depth

The depth of the change concerns the degree of change that can be absorbed without overloading the system. This is a problem for the Navy right now. They are currently establishing LRAs, but there is no rhyme or reason to their actions.

There is only one RA at DCMS. The Navy plans to grow to approximately 1,800 LRAs and if all of them suddenly gain the need to stand up overnight, there would be big problems in the Navy, especially at DCMS. [Ref. 17]

d. Publicity

Intra-Navy publicity is very important to the Navy's effort to implement DoD PKI. The reason is the lack of corporate knowledge in the area. Many people do not understand the concepts or the ramifications of PKI. Therefore, it is imperative that the Navy publicizes its efforts extensively in order to educate and familiarize its workforce to what is coming. [Ref. 17]

e. Supporting Structures

The last issue affecting enabling change is supporting structures. The Navy needs to invest in these structures. They will be the glue that will hold their connection to DoD PKI together. Who will answer the questions of the LRAs? How responsive will the RA be? Who will help the end user? These support structures will enable the change to move forward unfettered. [Ref. 17]

4. Reaction

One obstacle to change is people, specifically their reaction to change. To be successful, when the Navy manages the change effort, it must take into account the change's psychological effects on others. This reaction is usually greatest in those who have not participated in the decision process. And for the DoD this is usually the entire workforce. In the case of DoD PKI, very few people were consulted before the Under Secretary of Defense (USD) stated his desire for a DoD PKI. Therefore, a lot of people and services for that matter are trying to come to grips with the change. Often these

reactions to change are labeled resistance. Resistance to change is usually the result of three factors: inertia, habit, and comfort with the known. Inertia deals with people's routines. Things get done because they have always gotten done that way. This leads to habits. People become creatures of habit and then become very comfortable with the known. Change throws all of this out the window. It changes how people perceive their roles and responsibilities with in the organization. Because DoD PKI will affect all people, but only few participated in its decision-making process; there will be a high degree of resistance. This resistance will not be to PKI, but to their perceived loss of control. This is another reason the Navy needs to publicize PKI as soon as possible [Ref. 17]. This publicity will have the effect of educating the populace. And an informed populace is more likely to accept change than an uninformed one.

5. Trigger Events

Trigger events are large system changes that create new behaviors on the part of managers and workers [Ref. 17]. DoD PKI is a trigger event for the Navy. It will affect the over all information security system in the Navy and how people view security. In order for the Navy to understand this trigger event they must be in the proper mindset. "Mindsets direct attention to managing the puzzle, managing comparisons and analogies, managing symbols, and managing the conclusions and learnings as key challenges faced in trigger events." [Ref. 17] What trigger events do is bring peoples' mindsets into the arena of change [Ref. 17]. This is where the Navy needs to be. Before exhaustively focusing on implementation, they need to think about change and how they fit into the puzzle.

6. Mindsets

There are four mindsets that take place as the result of trigger events: assembly, conventional, amended, and evaluative. [Ref. 17]

a. Assembly

The assembly mindset occurs prior to the trigger event when rumors and small pieces of information are drawn together. In one sense this has already occurred in the Navy since the trigger event has already occurred. What most people are trying to do is develop a level of understanding with regard to the pending trigger event. Once the trigger event is self-evident the conventional mindset takes over. [Ref. 17]

b. Conventional

In the conventional mindset, people get involved with comparisons to the past and fairly simple, routine explanations [Ref. 17]. People really focus in on how the change will affect them personally. In the Navy, most people are unsure of the affects of PKI due to its lack of publicity and coverage. Their conventional mindset is based on what they have experienced in the past with regard to change endeavors. For the most part workers in the Navy are gun-shy. Some one is always trying to promulgate a change. When change isn't seen through, people get dulled to its importance. They are probably predicting that here. Once the trigger event occurs, the switch to an amended mindset is made. [Ref. 17]

c. Amended

In the amended mindset, people focus on before and after the trigger event. What was it like before the event? What is it like now? This is where the Navy is now. The trigger event has occurred, but people do not see any change yet. This is mainly due

to a lack of structure and funding. They think how will this affect my job. There will be some confusion as people come to grips with the change ramifications. People will adjust to the change over time and "hand-on experimentation, testing, and learning by doing are key" [Ref. 17] to this. The Navy will make great strides toward implementation if they provide a lot of hands-on demonstrations for people, do exhaustive system test before going online, and teach, teach, teach. They must educate the workforce. Once people have a symbolic meaning to the trigger event the evaluative mindset takes over. [Ref. 17]

d. Evaluative

In the evaluative mindset, managers and workers gain perspective. They evaluate the consequences of the trigger event in order to draw personal conclusions. Is this technology going to help us? Are we ready? This is a critical time because the results of the evaluative mindset are what future changes will be based against. If DoD PKI does not work, people will be apprehensive that the next system will work. There are many things managers can do to help their people and the organization through the four mindsets. [Ref. 17]

7. Managing Mindsets

Managers first need to manage puzzles. They want to provide information to dispel rumors or provide accurate information to workers. The Navy has done a fair job of getting the word to its information technology (IT) managers on how they will be affected. However, the word has not reached the most junior Sailor. Once the trigger event, in this case the memorandum directing DoD PKI, takes form the manager must manage analogies. The manager can provide analogies of past successes or how PKI

implementation is similar to another key security feature from the past. After the trigger event, managers mange symbols. Ceremonies help ease the transition pain and new routines and new rules take place. The vision of the change needs to be communicated so people understand what the organization is trying to do. Finally, the managers need to concern themselves with the conclusions and key learning points that resulted from the trigger event. The managers must find ways to evaluate the change. Are people signing their e-mails with their digital signatures? Are people losing their private keys? The mangers should very clearly state the significance of the event, i.e., we have added to national security by encrypting all sensitive but unclassified (SBU) and below e-mail traffic. [Ref. 17]

What people need is direction. When a major event like DoD PKI comes along it affects a lot of people. In order for the change to take affect people must adjust quickly and positively to trigger events [Ref. 171]. To do this people's mindsets must be considered. This portion of the chapter dealt with the forces that inhibit and create change. Our focus now is how to envision change.

B. ENVISIONING CHANGE

1. Vision

Almost everyone agrees that a well thought out vision is essential for change to be successful. However, there are many debates over what constitutes a thorough definition of vision. Regardless of what we accept as a definition of vision, vision has two components, a guiding philosophy and a tangible image. A vision gives us a sense of purpose and a reason for being [Ref. 17]. In contrast to vision is the concept of mission. A mission is shorter in duration than a vision and like a goal can be achieved. There is

debate over the attainability of a vision, in fact, some say that is why they are so essential. Visions make people keep their head and eyes on the horizon, instead of staring at their feet. This way they can see what is coming and can focus on their "final," yet unattainable goal. [Ref. 17]

In the Navy there are many overlapping visions. The vision for a DoD PKI is but one part of DoD's vision for information assurance and superiority. To be labeled "good" by Jick, the vision should be:

- Clear, concise, easily understandable
- Memorable
- Exciting and inspiring
- Challenging
- Excellence-centered
- Stable, but flexible
- Implementable and flexible [Ref. 17]

The problem with the DoD PKI vision is that some may not define it as a vision at all. The Under Secretary of Defense (USD) stated his desires clearly, concisely, and in an understandable manner, but he did not make his statements memorable, exciting, challenging, etc. The real key to implementing DoD PKI in the Navy will be the Department of the Navy Chief Information Officer's (DON CIO's) vision. Just because the Under Secretary of Defense (USD) and the DoD CIO do not espouse PKI as a vision, by no way hinders DON CIO or N6 from doing so. In fact, the success of the program may depend on it. PKI will be a huge change for the Navy and a vision will give the masses something to rally around. [Ref. 17]

2. Vision Statement

Vision statements focus on four elements: customer, employee, organization, and standards [Ref. 17]. For the Navy this means identifying its customers, internal and

external, and bringing their needs into its vision. Second, the vision must outline the importance of the worker and his role in the vision. For the Navy this includes letting every Sailor understand the importance of security and that they themselves are the weakest link in the information security chain. The organization is next. When we speak of organizations we mean their competencies, what they have achieved in the past. For the Navy this includes its rich military heritage of being an organization focused on information security. Finally come standards of excellence. By this Jick means those that appeal to the common worker and instill pride and resolve to protect, for example, the Navy's valuable information assets. In the end, what the vision statement does for people is tell them how things could be. Once the vision statement is drafted, it must be exposed, and that is the job of the visionary.

3. Visionary

The visionary is usually the person who crafts the vision. However, vision statements are not always drafted by one person much less "the person in charge". Sometimes vision statements are company wide exercises. The visionary must spend time telling the story, expressing the vision, and leading the troops. DON CIO should craft the Navy's PKI vision. DON CIO should do it with the help and assistance of the CNO (N6), CMC (C4I), and their staffs. That way the Navy and Marine Corps will assume part ownership of the vision, this may enhance implementation later on. Once the vision is written, DON CIO must go out and tell the story to the masses. DON CIO should attend workshops, visit commands, etc. He should become the ambassador for Navy PKI. He should draft disciples (CNO (N6) and CMC (C4I)) to his vision and encourage them to sign others on to the cause. Once the vision statement and visionary

have been identified, the next step is to garner the support and commitment of the organization to the vision. This commitment has four parts: communication, boundary testing, sign-on, and celebration. [Ref. 17]

4. Commitment to a Vision

a. Communication

Communication is the first key to garnering the support of the vision by the young Sailor. This communication takes the form of the visionary or his direct representatives physically presenting the vision to the people. In the Navy, the Program Manager for Information Warfare – Defend (PMW-161) under the guidance of the Director, Information Warfare Systems Directorate (PD-16), Space and Naval Warfare Systems Command (SPAWAR) performs this function. PMW-161 has a web site http://infosec.navy.mil and have run several workshops on PKI, but they are not reaching the masses. They do not appear to have the manpower or resources necessary to be the sole representative of CNO N6 for the Navy, much less DON CIO for the Department of the Navy. [Ref. 17]

b. Boundary Testing

Boundary testing is the next way to gain commitment to a vision. If a vision is poorly crafted or the visionary is not committed then this process will not be initiated. Boundary testing takes the form of individuals and organizations redefining their roles, jobs, relationships, etc. [Ref. 17]. In the Navy, this takes the form of training, experimentation, and task forces. With training, people are introduced to the vision and they learn what it means to them. For the common user, this will entail technical training, but also how they fit into the overall security protocol for the Navy.

Experiments are also great ways to test boundaries. People can test to see if the new technology works and the organization can see, if in fact, it is increasing security. Lastly, task forces can be set up to see how the vision is being accepted. They can gauge the pulse of the organization and help to pass the word. They can also provide another means of training and support. [Ref. 17]

c. Sign-on

After the organization begins committing itself to the vision, the process of signing-on its members begins. This entails the individual commitment of Sailors toward ensuring information security in the years to come. A leader can not "truly" force someone to sign-on. This is because the act of physically signing-on, i.e., signing a security memorandum, is a purely symbolic gesture. What the Navy needs is a psychological signing-on, where the Sailors embody the ideals of signing-on to the vision. Sailors should be made to feel it is their decision to sign-on. Leaders must be patient and continue to "preach the vision." They can develop slogans, "Information security, it starts with you and PKI," or develop buttons and stickers. Whatever the medium, the idea is to lead the horse to water and let him choose to drink or not. This way sign-on is personal and people will internalize it. [Ref. 17]

d. Celebration

The last process of getting commitment to a vision is celebration. This is done to exemplify successes and sends out the message that actions that support the vision are important. The Navy can do this through additional days off, parties, etc.; people like to be recognized. Organizations with high sign-on and no public key security problems should be rewarded accordingly. Once these four commitment to a vision

issues have been adequately addressed, the Navy should be well on its way towards successfully implementing the vision. As a side note, there will be those that do not want to play. Tough decisions will have to be made, i.e., reassignment, retraining, retiring, and/or termination. [Ref. 17]

5. Alignment

This commitment to the vision has the affect of aligning the organization toward a common goal or vision. One is aligned to their job to the degree they do what they are supposed to, they enjoy doing it, they interact well with others, and please the boss [Ref. 17]. If some one in an organization is an aligner they are trying to "enlist support for a change" [Ref. 17]. This is what the Lieutenant and Lieutenant Commanders in the Navy need to do. They need to bring the idea of public key cryptography and digital signatures to their people.

6. Dissatisfaction

One last thought on envisioning change is how to create an environment ready for change. A crisis usually does the trick, but leaders do not want to play this card too often or their people will think they are crying wolf. Instead leaders need to instill a sense of dissatisfaction. What this means is that the leaders, i.e. DON CIO and CNO N6 must honestly be dissatisfied with the way the Navy secures its SBU and below information. They must then create an environment where their dissatisfaction is diffused to the Sailors throughout the Navy. [Ref. 17]

The first way this can be done is by sharing competitive information. By doing this you symbolically show the people a way of building trust. The Navy could do this by actually showing the statistics for web site attacks, security breaches, and types of

information lost. This makes information security real and infuses a sense of, "Hey, our current system is not working," in the minds of every Sailor. [Ref. 17]

The next way to diffuse dissatisfaction is by pointing to poor examples of individual, on-the-job behaviors. If individuals know their behavior is unacceptable, maybe then they will correct themselves. When PKI is finally implemented in the Navy, there will be those Sailors who "keep" losing their private keys. Peer pressure and discipline will need to be brought to bear on them. [Ref. 17]

Showing the Sailors just how far the Navy is from their goal is another means of diffusing dissatisfaction. The Navy could establish an award for security excellence and create a model for others to evaluate themselves against. Regardless if a unit is inspected annually or not, they would always have a metric to evaluate their information security posture. [Ref. 17]

The last way to instill dissatisfaction is by mandating it. This has some draw backs, since people will not feel "free" to sign-on. This could lead to the belief that we have to change and people will not internalize the change. One way around this is for the Navy to say it is only going to deploy or fund activities that have full-fledged information security systems. And then those that did not get funding or were not deployed would not be directly penalized, per se; instead they would determine their own fate. [Ref. 17]

The key concept is that not one, but a combination of the four diffusing strategies needs to be employed to successfully diffuse dissatisfaction. If dissatisfaction can truly be achieved, then people will rally behind the shared vision. And once a vision is shared, the road to implementation can begin. [Ref. 17]

C. IMPLEMENTING CHANGE

Implementing change in an organization is a complex topic. To get a feel for the problems involved, the following "hows" should be pondered:

- How do we get the organization to change?
- Here is how we will go about changing.
- How are we doing?
- How are people responding to the change? [Ref. 17]

To answer the first two "hows" the Navy needs to apply techniques. These take many forms, i.e., web sites, tutorials, seminars, etc., but it is the consistency of the message, which is of main concern. To ensure consistency and answer the third "how" the change process must be monitored. This monitoring must take on a tangible form. For the Navy, this could consist of the number of web sites or the amount or type of information intercepted from e-mails over the Internet. By measuring implementation progress quantitatively, evidence is created for resonance justification. The last how is answered by insuring your implementation effort focuses on the people. Implementation efforts must be flexible. They must have the ability to change course or back track as conditions change. Do not force a square peg into a round hole. [Ref. 17]

1. Change Participants

When an organization is setting itself for change, its work force can be divided into three categories: change strategists, change implementers, and change recipients. Change strategists develop the vision of change. They see the future face of the organization. Sometimes they plan the implementation of the change with programs, policies, etc. At other times they rely on the change implementers to plan the change. The change implementers "make it all happen." They try to keep the change true to the vision. They work closely with strategists and the recipients. The change recipients are

the ones who must accept the change. This behavior in large part determines if the change will succeed or not. [Ref. 17]

2. Implementation Problems

When the strategists or implementers are starting their implementation planning they need time early on to learn from others past mistakes. It is easy to get locked on to the change vision and never see what else is around you. A lot of organizations have changed over the years and a lot of research has been done on the subject. Some factors worth considering are:

a. Time

Implementation often took more time than was expected. In the military, things also seem to take longer to get done than expected. This is due mainly to its size and diversity. [Ref. 17]

b. Problem Areas

Many additional problems surfaced during the implementation process that were not previously planned for. It is difficult to plan for everything no matter how hard you try. [Ref. 17]

c. Coordination

Effective liaison and communication between implementers did not exist. Liaison between task forces must be made and their message must be consistent. [Ref. 17]

d. Competing Activities

Crisis and daily business usurped the power and inertia of the implementation. This is business as usual in the military. Operations often and regularly usurp change implementation. [Ref. 17]

e. Capabilities

The implementers did not have the skill set required to implement the change. The trainers need to be trained first. [Ref. 17]

f. Training

The change recipients did not receive adequate training. Time and resources must be allocated to train all personnel. [Ref. 17]

g. Outside Factors

Politics, economics, or other outside forces. Different leaders have different priorities. There must be consistency to the vision and message that all Sailors receive. [Ref. 17]

3. Tactical Implementation Steps

There is no clean recipe for change, but as implementers continue their planning there are some general rules to assist them:

a. Analyze the Organization and Its Need for Change

When the Navy analyzes itself, it should take into account its history of resistance to change. It should start small, i.e., one regional information technology service center (RITSC) at a time. If PKI works well in one area, i.e., San Diego, then expand. The Navy needs to make its plans clear to all involved. PMW-161 has a web site, but its usefulness is unknown. One way the Navy could help itself is by receiving

feed back from the Sailors in the fleet. The Navy would then be able to define what their problems are and who the main users of PKI will be. [Ref. 17]

b. Create a Shared Vision and Common Direction

The Navy can unite its forces behind the PKI process by outlining the need for it. It needs to explain why it is implementing it and what the ramifications are if it does not succeed. [Ref. 17]

c. Separate from the Past

The Navy needs to clearly show that current SBU and below information is easily compromised. They need to show that PKI will not work if the Navy continues to use its past paradigms. [Ref. 17]

d. Create a Sense of Urgency

If the Navy can create a sense of need in its populace, then the implementation will go much more smoothly. [Ref. 17]

e. Support a Strong Leader Role

DON CIO and CNO N6 must be strong advocates for the movement to adopt DoD PKI Navy wide. [Ref. 17].

f. Line up Political Sponsorship

The Navy and DoD must show this is important by allocating resources and this includes money for smart cards, readers, training, etc. Nothing will derail the change effort more quickly than forcing a change and then having the commands pay for equipment and training out of their O&M budgets. [Ref. 17]

g. Craft an Implementation Plan

The Navy should have a specific plan for implementation. They currently have a version of that titled DON Medium Assurance (Class 3) PKI. Recommendations regarding this document are located in Chapter IV [Ref. 17].

h. Develop Enabling Structures

The Navy must enable the change by hosting workshops (they have done this in the past), start up a test scenario (standing one RITSC initially, i.e., San Diego), and provide a reward program, perhaps monetary unit awards. [Ref. 17]

i. Communicate, Involve People, and be Honest

DON CIO, CNO N6, and the implementation task forces need to clearly state the vision, involve everyone, and be honest. They need to tell it like it is. [Ref. 17]

j. Reinforce and Institutionalize Change

The leaders need to reward successes and reaffirm the new secure information culture, i.e., DoD PKI. [Ref. 17]

4. Basic Concepts of Organizational Change

So far this paper has addressed the pitfalls to avoid when implementing change and provided a general implementation outline. The nuts and bolts of change address how people think and why they think that way. Organizations like the Navy are complex systems. They have their own environment, resources (people, equipment, bases, etc.), and a long a gloried history. Figure 5-2 is the model used to describe organizational change. [Ref. 1]

The diagram describes the two basic concepts of strategy and organization. Strategy is the pattern of decisions determining the allocation of resources over time in

response to environmental stimuli. In the case of the Navy implementation of PKI the resources are training, personnel, dollars, hardware, and software. The outside stimuli are DoD PKI and the Under Secretary of Defense. The organization is the force that changes strategy into output. Strategy is outlined above and output is a fully enabled Navy implementation of DoD PKI. [Ref. 17]

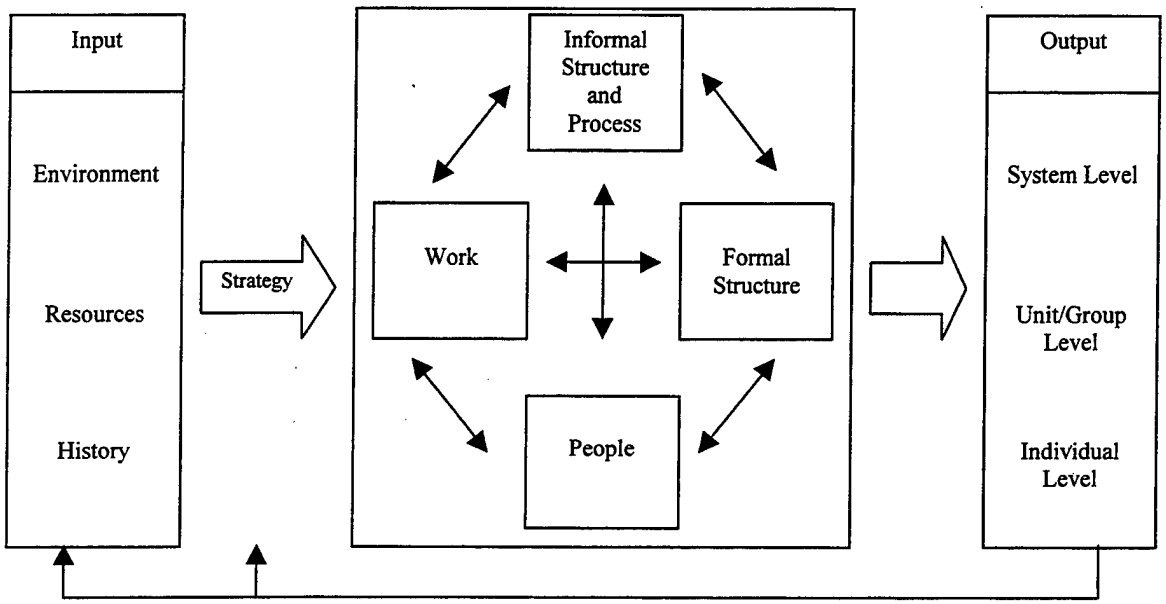


Figure 5-2. Organizational Change [From Ref. 17]

In order for an organization to get output it must bring to bear its core components of work, people, formal strategies and processes, and informal structures and processes. These components need to be in congruence. The strategy must be consistent with the environmental conditions and there is fit among the core components. [Ref. 17]

In order to bring about change an organization needs to use one of its core components. When bringing about change the whole concept of congruence may change. There are three issues, which should be addressed when managing change like this:

a. Managing the Political Dynamics Associated with Change

To the Navy this means getting a handle on the politics of PKI. One issue is the trust of the employees when it comes to certificate key escrow and another is the ownership of RITSC facilities. If the Navy can not handle the politics of PKI, then the system will not work. [Ref. 17]

b. Motivating Constructive Behavior in the Face of the Anxiety Created by the Change

The Navy needs to positively sell the concept of PKI. By doing so, they can keep anxiety low. [Ref. 17]

c. Actively Managing the Transition State

The Navy can not simply dump the responsibility for PKI implementation into the hands of the major claimants. They need to teach, educate, and help people through this process. [Ref. 17]

Because change in the Navy is a large-scale endeavor, certain characteristics often come into play. The first is multiple transitions. The DoD is planning for an incremental implementation over several years. The next is incomplete transitions. The Navy needs to ensure previous transitions are complete before they move onto the next one. Then come uncertain future states. The Navy should not get locked on to a vision of the future. It should remain flexible and adjust their vision as technology changes with time, especially smart cards. The last characteristic is transitions over long periods. It will be hard for the Navy to continuously manage a change of this magnitude over the 3 – 5 years it will take to fully implement DoD PKI. Given the frequency with which people

move and the degree, to which implementation efforts can wax and wane over time, the Navy should plan accordingly. [Ref. 17]

5. Types of Organizational Change

The Navy is undertaking a large-scale organizational change. In order for the Navy to understand what this means it should understand change. Change has two parts, scope and positioning. [Ref. 17]

The scope of the Navy's change is the degree to which subsystems will change in relation to the entire system. The change proposed here affects the Navy's information assurance (IA) subsystem. This is a strategic change. It is strategic because is affects the whole organization and every person. Every person in the Navy is going to carry a smart card with their two private keys (identity and certificate) on it. This is a huge change for people. This will develop a new congruence for the Navy. [Ref. 17]

The second part of the change is the positioning of change in relation to key external events. The key external events the Navy is planning for are called anticipatory changes. These changes are cyber terrorism and the vulnerability that comes with sending 95% of the Navy's SBU and below information over public Internets. As a result of the Navy's strategic and anticipatory change, its overall change is classified as reorientation, see Figure 5-3. [Ref. 17]

	Incremental	Strategic
Anticipatory	Tuning	Reorientation
Reactive	Adaptation	Re-creation

Figure 5-3. Types of organizational Change [From Ref. 17]

Reorientation is the class of change that involves a fundamental redirection of the organization. In this class, links to the past are emphasized [Ref. 17]. This is true in the Navy. Information assurance has always been important, but in the past most information flow was paper. Now as the world moves into a digital paperless society with the Internet pervading all we do, it is so important that we make a fundamental shift in information security. This is what PKI does for the Navy. Reorientation can be viewed in relation to its intensity and complexity. The intensity is the severity of the change that is felt by the organization and the complexity deals with the organization itself. The more dramatic the change and the more complex the organization the greater the complexity and intensity. In the Navy, the intensity is fair since we are not talking about IA for the first time and complexity is also fair due to the traditional hierarchical structure of the Navy. Because the change has a strong link to the past, but still fundamentally changes the organization, reorientation is called frame-bending. [Ref. 17]

6. Organizational Frame Bending

Frame-bending consists of four principles: initiating change, content of the change, leading change, and achieving change. Each principle has two or three sub-principles. Together these principles and sub-principles, see Figure 5-4, describe how the Navy can implement DoD PKI effectively. [Ref. 17]

a. Initiating Change

Initiating change describes how to get change going. It has three sub-principles: diagnosis, vision, and energy. When diagnosing an organization one is determining what parts of an organization must change in order for the change to be effective. For the Navy, this includes getting everyone involved in the technology. A

technologically advanced Navy is the vision of the future. PKI is, but one part of the future vision. The Navy and other services have large hurdles to overcome here. They provide low pay and have shrinking budgets, yet they want young, energetic, bright people in their organizations. This is a problem. [Ref. 17]

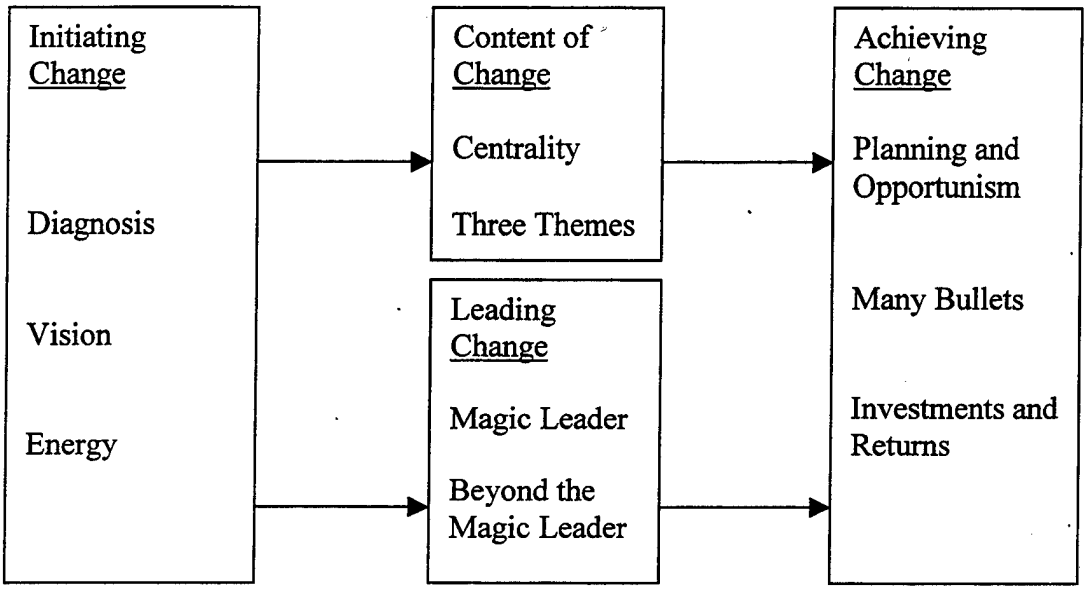


Figure 5-4. Organizational Frame Bending [From Ref. 17]

To properly implement change, one must move from one state to another. In doing so, there needs to be a guiding vision. For the vision to successful it needs to be:

(1) **Rationale.** The Navy needs to tell its people why this change is needed.

(2) **Stakeholders.** The Navy needs to address the Sailors, who are the stakeholders, and their efforts toward this are crucial for future successes.

(3) **Values.** The Navy needs to drive home its core values of honor, courage, and commitment.

(4) **Performance Objectives.** The Navy should define for everyone what will be considered acceptable performance by organizations and individuals once the change is affected.

(5) **Organizational Structure or Processes.** The Navy should emphasize the Navy Marine Corps Intranet (NMCI) and how PKI and it will provide IA and network effectiveness into the future.

(6) **Operating Style.** The Navy should address how people will interact. The culture of teamwork and cooperation should be stressed. In many ways visions are simply symbolic, but that is often a good thing. It gives people the ability to hang their hat on something that is tangible and will be around for awhile.

Change implementation is most successful if it can tap into the energy in organizations. Organizations traditionally strive to stay stable and therefore have a lot of energy to resist change. In order to overcome this resistance, the Navy needs to create a sense of urgency. They need to show the Navy, from the CNO to the Seaman Apprentice, why the Navy and they must adopt this new technology and why they must use it religiously. Once change is initiated, it is time to define the content of the change. [Ref. 17]

b. Content of the Change

The content of the change principle is made up of the centrality and three theme sub-principles. [Ref. 17]

Centrality deals with ensuring the change required is linked to the strategic goals of an organization and its members. The Navy can do this by showing the content

of the change in relation to the Navy's defense in depth policy. It must bring this understanding to all involved. [Ref. 17]

The three-theme sub-principle deals with the human side of change. Change saps a lot of energy from people. It is important to understand that the average manager can handle only three change efforts simultaneously. The Navy usually has multiple changes, which affect multiple systems, running simultaneously. The Navy needs to ensure that PKI implementation is one of its top three change efforts or it may not succeed as planned. [Ref. 17]

c. Leading Change

Leading change has two parts: Magic Leader and Beyond the Magic Leader. [Ref 1]

The "Magic Leader" is the person who serves to rally the troops and who portrays a "magic" feel. He energizes the masses toward the change. These magic leaders tend to have the following characteristic:

(1) **Distinctive Behaviors** – leaders envision, energize, and enable change in their actions. [Ref. 17]

(2) **Ability to Create a Sense of Urgency** – leaders show the significance for the change. [Ref. 17]

(3) **Guardianship of Themes** – leaders ensure the change lives on. A lot of change efforts die over time because its champion does not follow through. [Ref. 17]

(4) A Mix of Styles – leaders must show various management styles. By doing this they can appeal to the masses by adjusting their approach to

their audience. One probably would not use the same approach talking to Seamen and engineers. [Ref. 17]

Having a "Magic Leader" is not enough. There must exist a foundation for success. [Ref. 17]

The "Beyond the Magic Leader" sub-principle states that a foundation of followers and subordinate leaders is crucial toward change success. Early on the DON CIO and CNO (N6) must develop disciples who can continue to pass on the word. In addition, a group of followers must be garnered. This creates a base for the Magic Leader, but more for his disciples to grow on. As more and more Sailors believe, the change becomes more tangible. [Ref. 17]

d. Achieving Change

The last part of frame-bending is achieving change. This involves those implementation steps that ensure change takes hold over time. Achieving change consists of planning and opportunism, many bullets, and investment and returns sub-principles. [Ref. 17]

In planning and opportunism, the Navy needs to create detailed plans on how to change. The author of this paper has outlined ideas on how to implement change in Chapter IV. The important point is that plans will change. The leader and his staff must stay flexible and adapt as the situation warrants. [Ref. 17]

The many-bullets sub-principle states that change must occur over many avenues of approach. Newspaper, video, web sites, workshops, and task forces should all be employed to change the culture of an organization. Because large organizations are

especially resistant to change, i.e., the Navy, many different ways should be utilized to garner change. [Ref. 17]

Lastly, the investment-and-returns sub-principle deals with the amount of resources and effort required to instill change. There are two subparts to this principle called: no-free-lunch and check-is-in the mail. [Ref. 17]

In the no-free-lunch hypothesis, it is very clear that without significant investment in time, manpower, and money, change will not occur. This is an area that concerns the author with regards to the Navy. The Navy has not committed the manpower, i.e. PMW-161 (one man) or resources (money for implementation) in their plan. Without such a commitment the end state is questionable. [Ref. 17]

The check-is-in the mail hypothesis states that as the complexity of the organization increases, so does the time required to change. In the Navy, this can be seen in its NMCI efforts. Many commands operate their own WAN. Each maintains their own infrastructure, personnel, and equipment. Most agree NMCI will be more efficient and cost effective, but no one wants to take the first step and give up their assets. [Ref. 17]

The Navy will go through several states as it implements this change:

- Awareness – Sailors will become aware of the need for PKI and what it entails.
- Experimentations – Pilots will begin to see really what implementation requires.
- Understanding – As the results of experimentation are known, Sailors will learn the true scope of the change.

- Commitment – DON CIO and CNO (N6) need to take affirmative steps to ensure change.
- Education – Implementers and the Sailors need to learn the skills necessary to make the technology a success.
- Application leveraged issues – New skills and people are applied to leverage success, i.e. RITSCs manned as RAs and help desks operating 24 X 7.
- Integration into on going behavior – The end state. People believe in and use PKI in everyday situations. It becomes part of the culture and the norm.

7. Developing Change Process

In order for change to be successful their must exist a shift from programmatic change toward task alignment. In programmatic change the change focused on the knowledge and attitudes of individuals. However, in task alignment the focus is on the organizational roles that Sailors play. "The most effective way to change, behavior, therefore, is to put people into a new organizational context, which imposes new roles, responsibilities, and relationships on them." [Ref. 17] This in essence forces new attitudes and behavior on Sailors. This process has three parts: coordination, commitment, and competencies. [Ref. 17]

Coordination between those using PKI services, all Sailors, and their trainers is critical. People must be free to ask and learn as the process moves forward. There must be a strong commitment from the top to ensure the coordination exists. The competencies or skills required to make the technology a success must exist too. Without these factors, coordination, commitment, and competencies, the change effort will falter. [Ref. 17]

Successful companies are moving away from programmatic change to task alignment. Task alignment is the reorganization of workers and their roles and responsibilities to solve specific problems. Task alignment is different in large organizations, but there are six steps toward implementation: [Ref. 17]

- Mobilize commitment to change through joint diagnosis of business problems – The Navy should involve all levels in the implementation planning process. This way they will find out what the hurdles really are.
- Develop a shared vision of how to organize and manage for competencies – The Navy should expand its group of change strategists and implementers and train them with the required skills for implementation. Once trained they should be sent out to share the vision and importance of the change.
- Foster consensus for the new vision, competence to enact it, and cohesion to move it along. The Navy should follow up with training for all hands on how the technology works and how to apply it. This will build consensus for the vision and competence in PKI.
- Spread revitalization to all departments without pushing it from the top. The organizations where PKI is being employed; which is all organizations, must have the infrastructure to support it. There must be commitment at the operational level.
- Institutionalize revitalization through formal policies, systems, and structures. The Navy must invoke policy and procedures so PKI will survive after the task forces and the implementation period ends.

- Monitor and adjust strategies in response to problems in the revitalization process. The Navy's goal from this process was to learn to adapt to a changing environment. There is increasing importance on the Internet and therefore the Navy is more vulnerable. Hopefully, the Navy will learn what it needs to help it adapt in the future.

Hopefully the "hows" have been properly addressed. Implementing change is a truly complex topic. It cuts across all borders, affecting people, policy, politics, etc. One portion of this equation deserves further examination – people. For people are the recipients of change and that means a lot.

D. THE RECIPIENTS OF CHANGE

So far this paper had addressed how to design and implement change programs. However well crafted, these programs affect a certain group of people – the recipients of change. What the author intends to do is show how change can be introduced, once the consequences of change, and its affect on people, are brought into the light.

1. Reaction to Change

One of the first things to realize about change is that people take it personal. People like the status quo. They do not like to have their boat "rocked". And this is exactly what change does. In its most basic form, change can only succeed when people themselves change. As an example, PKI will cause people to view information security from a different perspective. Non-repudiation will legally hold them accountable to their words. The concept of key escrow will give some people the feeling that "Big Brother" is watching. This may cause some people to distrust PKI. These are examples of people's reactions to change.

Reacting to change is a personnel endeavor. Everyone does it differently. There are two basic concepts that most deal with control and energy. Control deals with an individual's surroundings. As time passes an individual settles into a certain work pattern or group of habits. As change is introduced the individual internally determines if the change affects them and if it does not, they do not worry. However, if it does, do I have "control" over it or it over me? The more control it has over the individual the more negative the reaction to change. People feel threatened by what they can not understand or do not know. Change programs are often foreign to the lowest levels of an organization. This will be true in the Navy when the Seaman Apprentice is handed a floppy disk and told, "This is your private key. Protect it, it is very important." People's reactions to change cost them energy. [Ref. 17]

This energy is the energy to deal with the change and possibly to deal with the individual's reactions to change. This can enact an enormous toll on people. Even when people like the change, they must be given time to adapt. People must be given space to assimilate, understand, and "fit" the change into their lives. This has always been difficult for the military. An edict will come down from on high on Monday and everyone will be expected to be on board by Friday. This just discounts the value of people and their feelings and needs. [Ref. 17]

In order to adapt to change people must move through a set of psychological transition stages: ending phase, neutral zone, and new beginnings. [Ref. 17]

In the ending phase, people let go of their previous process. In the Navy this will mean, how people send e-mail, how they access web sites, and how they view their communications. There is a lot of pain and frustration during this phase. The second

phase is the neutral zone. In the neutral zone people have left behind their old way of doing business and not yet accepted the new way. They are in "no man's land". They are essentially mustering enough energy to continue forward with the change process. [Ref. 17]

Once enough energy is built up, people enter the new beginnings phase. In it, people align themselves with the vision of change. They accept new ways of doing things and the change takes root. The military tends to force people into this phase and forget about the ending and neutral zone phases. They usually send out naval correspondence, make presentations, etc. all in the effort to get people on board. However, what people really need is time to deal with the change. If people view the change as positive and they have time to go through the transition stages, then change can occur. [Ref. 17]

Organizations have a vested interest in the change effort. And as such, they expect results. This causes them to react with impatience. When the workforce is not in the new beginnings phase almost immediately. One can understand the organizational response. In the first two phases people are not nearly as productive as before the change or in the new beginnings phase. As such, it becomes difficult for companies to stand by and watch their employees do nothing. And they intensify their efforts with more pep rallies, presentations, etc. The problem is people view this additional push as more control. They therefore require more time for change.

The author proposes the Navy initially present the concept of DoD PKI to the masses early on. They should provide the masses with literature and web sites and then they should stand down. They should focus on training preparation and infrastructure set

up. And then six months later initiate the push toward full stand up. This would in effect, introduce all Sailors to PKI and then give them a chance to move from the ending phase to new beginnings. The web sites and literature would help educate the individuals when they were ready to learn more. The six months off would give people their time to cope with change.

There are ways the Navy can help people during this period of transition. They could:

- Keep your cool in dealing with others.
- Handle pressure smoothly and effectively.
- Respond nondefensively when others disagree with you.
- Develop creative and innovative solutions to problems.
- Be willing to take risks and try out new ideas.
- Be willing to adjust priorities to changing conditions.
- Demonstrate enthusiasm foe and commitment to long-term goals.
- Be open and candid when dealing with others.
- Participate actively in the change process.
- Make clear-cut decisions as needed. [Ref. 17]

As stated earlier, organizations can help people deal with change, but individuals have an equally important role in the endeavor as well. People need to cope with change. Having said that, some people have deeply emotional reactions to change. Dealing with change cost them energy. And any negative reactions to change cause then more energy. This saps people's strength. In order to help themselves cope; people must give themselves permission to feel these emotions. In other words, its okay to be mad, sad, or depressed. Do not fight the emotions or you will further sap your energy. In fact, the best way for people to react to change is to let things run their course. In order for people to regain control, people should manage stress. [Ref. 17]

Managing stress consists of:

- Maintaining physical well being.

- Seeking information about the change.
- Limiting extraneous stressors.
- Taking regular breaks.
- Seeking support. [Ref. 17]

Taking care of your physical well being entails diet, exercise, rest etc. And it gives you some control over your environment. By seeking information about the change you are developing a sense of objectivity that will help you organize your contextual image of the change and thus help you control the change. One can also seek the support of others. It is often helpful to find a group with common experiences. This give you control because you do not feel isolated in your emotions. [Ref. 17]

The last way individuals can help themselves cope with change is to exercise responsibility. In doing this people:

- Identifying options and gains.
- Learning from losses.
- Participating in the change.
- Inventorying strengths.
- Learning new skills.
- Diversifying emotional investing. [Ref. 17]

Each individual needs to establish a foundation from which to stand. This foundation consists of those parts of your life that are secure, i.e., family, friends, hobbies, etc. From here one can see the change from a different light. This helps people gain perspective. So does reevaluating oneself. By doing this, people understand where they are in relation to the change. They find out how they can participate and what their strengths are in relation to the change. Individuals can do a lot to help themselves cope with change, but their managers can help as well. [Ref. 17]

Managers can help their employees by rethinking resistance, giving first aid, and creating the capability for change. [Ref. 17]

In rethinking resistance managers view of resistance is changed. Currently, managers think of resistance as an obstacle to over come. Instead they should think of resistance as the first step toward implementation. Managers should focus on the motives and sources of resistance. By focusing here the manager can help employees through the change process by removing obstacles from their path versus forcing them over a hurdle. [Ref. 17]

In giving first aid, mangers need to focus on their people. They need to take the time to listen to their employees. This will go along way toward helping people cope with change. Often people just need an outlet for their frustration and when they finally talk to someone, they finally verbalize what they perceive to be a problem. Yet managers support their concerns and hopefully show them that it in fact is not a problem, but an opportunity. This is, of course, more easily said than done. [Ref. 17]

In creating the capability for change, managers help people achieve change and encourage them to feel good about the change. This entails taking risks and can be accomplished through safety and rewards. With safety, people are provided assurances that taking risks toward the change will be supported. And with rewards people are given promotion or monetary awards for taking the risk toward change. [Ref. 17]

Change is not a foreign concept to most organizations and people. In fact, both seem to undergo change continuously. In certain circumstances we are change recipients and in others we are change agents. In both cases there is a mutual responsibility between organizations and people to cope with change. They both have responsibilities and they both must be aware of and sensitive to the others' needs. In the end, change will always exist and probably continuously at that. Therefore, it is imperative that

individuals and organizations invest in the emotional and physical skills necessary to continually adapt and grow. [Ref. 17]

E. CHANGE AGENTS

What is a change agent? There are many different answers to this question. This author's definition is that it is an individual or group that assists their organization in arriving at a future state. They can envision this future state, at least in their own context, so they can help the organization to move toward it. Change agents are apt at implementing the change. They do this well because they have a strong belief in the organization and a desire to further it. And finally, change agents are recipients of change as well. Because they are almost always not the visionaries who initiate change, they must change themselves before they can change others. [Ref. 17]

Throughout the course of change, change agents will undergo some positive and negative emotions. The negative emotions are resistance, frustration, loneliness, and pain. The positive emotions are challenge, teamwork, personal growth, and gratification. [Ref. 17]

The most universal of all the negative emotions is resistance. This resistance can come from above, below, or from the sides (peers). The reasons are many, but one reason is the competing constituencies with in an organization. Each has its own agenda and often, if not always, these agendas are different. Frustration comes from all directions as well. Change almost always takes longer than expected and the motivation for change wanes over time. Inevitably, there are low points that must be weathered in order for change to take hold. Change agents, almost by definition, are the leaders of the movement. And as such, they encounter problems and obstacles well before anyone else

can identify them. This whole process can be very isolating. Change agents often experience loneliness. They often feel they have no one to turn to for companionship. The life of change agents is also riddled with pain. This pain comes form people having to change their routines and ways of doing business. It also comes in the form of layoffs and reorganizations. These significantly affect people's lives and change agents feel the pain of the people. With all these negative emotions encompassing a change agent's life, why would anyone become a change agent? The answer to that is the flip side of the coin or the positive emotions associated with change. [Ref. 17]

Many change agents are drawn to the challenge of change. Some people's psyches thrive on chaos or on putting the pieces of a puzzle together. When given the opportunity to drive change, these people rise, excitedly, to the occasion. One person seldom accomplishes change. Usually groups of change agents come together to work as a team. This creates an atmosphere reminiscent of little league baseball days. All the kids join together in conquest of a common foe. This can be very uplifting for some. Going through change causes people to do a lot of soul searching. People must look with in, in order to find the strength and skills required to make the change effort succeed. Whatever doesn't kill us makes us stronger. This adage applies to change agents and their personal growth during change. Finally, change agents often experience gratification. This occurs as a result of big and incremental successes. When one ship finally establishes their LRA and finishing enrolling all its Sailors. When NMCI finally reaches maturity and the Navy actually experiences economies of scale. The life of a change agent is obviously riddled with emotions, some up and some down. [Ref. 17]

Change agents have to deal with a variety of influences as they go about their tasks. One of the dominant forces is the culture of the organization. The stronger an organization's culture, the harder it will be to institute change. This of course is true only if your change goes against culture. The strategy the change agent employs will have to depend on the culture he/she finds himself in. This culture extends to the national culture as well. The U.S. holds more of an instrumental view of organizations. "...The organization is perceived primarily as a set of tasks to be achieved through a problem solving hierarchy, where positions are defined in terms of tasks and functions and where authority is functionally based." [Ref. 17] This culture is opposite the social view of organizations. The social view is held in Latin cultures. "...The organization is primarily conceived as a collectivity of people to be managed through formal hierarchy, where positions are defined in terms of levels of authority and status, and where authority is attached more to individuals than to their offices or functions." [Ref. 17] These two views show that organizations think and act differently as a result of their national culture. Therefore, when developing change strategies, change agents must take this in to account. Different change strategies will be required in different cultural environments. The change agents' job is therefore compounded. One solution, obviously, does not fit all. The change agent must understand the cultural context of the change as well. [Ref. 17]

How is a change agent supposed to do all this? One answer to this question is through empowerment. Change agents do not take on the role of Lone Ranger; instead they take on the role of professional baseball manager. Why professional? Because at the Major League level all players, as in the military, are professionals. As such, they are

expected to do the right thing. Why manager? Because he is the one who guides the team, changes pitchers, and calls for specific plays, but does none of the actual work himself. When the culture of an organization is such that people feel empowered to create change, competitors better watch out. In the future, we will all be change agents. All of us will understand our role in the organization and how it affects the whole. We will realize that the competitive market place is not for slouches. We must all identify and initiate change in order to continually fine-tune the organization. Managing change can be thought of as being a kin to fostering creativity. People are free to find weaknesses and empowered to enact creative solutions. [Ref. 17]

Most change agents in today's organizations are in middle management, i.e., LTjg, LT, and LCDR. As such, they have an interesting and powerful place in the organization from which to manage change. This place is called the middle space, see Figure 5-5. It is the place that pulls us between other spaces. [Ref. 17]

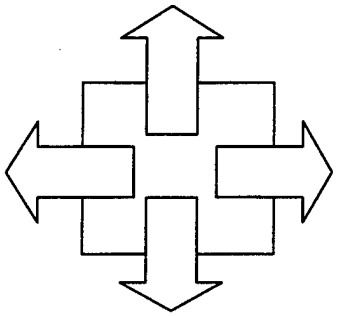


Figure 5-5. The Middle Space. [From Ref. 17]

Often we are pulled from above, below, and from our peers on our sides. The pressure in the middle space is intense. Each space has its own competing agendas. They want you, in the middle, to solve their problems. However, in fact their problem is not with you at all, but the one to your left, right, top, or bottom. What we need to do is

facilitate the top and bottom, primarily by getting them together and helping them come to a resolution. The middle's place is not to solve their problems. One must strive to "stay out of the middle" and compress the organization to ease and speed up decision-making. [Ref. 17]

There are two strategies and five tactics for being a change agent in the middle. The first strategy is to not let yourself be pulled into the middle of other people's problems. Resist the temptation from above and below to solve other people's problems. Instead, act as a facilitator and get the parties together. The second strategy is to not lose your mind. A change agent in the middle will be constantly torn. He will be drawn to both sides and will embrace parts of each objective. One must maintain objectivity and focus on what needs to be done. We need to develop a unique middle perspective. This perspective will allow us to vision a future state for the organization. [Ref. 17]

Once these two strategies are set we need to embrace the five tactics. The first tells us to be top when you can and take responsibility for being top. This means do not let the bottom escalate the problem to top. If you can fix the problem, then do so. It is easier to ask for forgiveness, than it is to ask for permission. The second tactic is to be bottom when you should. This means do not pass on bad ideas and issues. If you can fix them, then do so, but if its just garbage, send it back to top and explain what will happen if you send this down. The third tactic tells you to be a coach. Listen to top and bottom. Support their needs and let them know you care. Just listening is all some people want. Its amazing how much it can accomplish. Once this is done you can facilitate top, bottom, left, or right. Help each side understand each other's views. Once this is done true progress can be made. The last tactic is to integrate with one another. Change

agents can learn a lot from their peers. Find out what works for Bob, or talk to Alice and get her feedback. When the middles join together they form a powerful coalition. This coalition gains and shares knowledge of the organization, thereby constantly increasing its power. This power can then be used to influence large numbers of people and institute change. This is where the true power of being in the middle as a change agent comes in to play. [Ref. 17]

One way to bring about change like PKI is to set out a task force with "almost" unlimited power. Their mission would be to cut across hierarchical boundaries and cultures and identify impediments to change and enact solutions. They could call any and all resources to bear to solve problems. The command hierarchy has to support the team completely. The team could be crafted by DON CIO and blessed by the Secretary of the Navy, CNO (N6), and CMC (C4I). They would have the power to make things happen. These would be the true change agents. The problem is that the military is an extremely large political bureaucracy. And as such, no one has shown the fortitude to make the necessary changes with any sense of urgency or and in a timely manner. [Ref. 17]

Change agents are an important part of change movements. They take on many responsibilities. One is visioning the future state. As such they must understand their character and develop a course to get the organization there. This is the CIO's job with PKI. The author believes the CIO's staff or a task force should be set up to carry out the tasks required. One of the important parts of change is training. Training is one facet of a change agent's agenda. The change agent creates a plan, visions a future state, and empowers and trains the masses. Training is critical because skill sets are crucial and

perishable. Not only must the training be thorough it must be followed on with hands on practical experience. This is where PKI has a problem. The Navy can not certify two or three people with collateral duties as LRA administrators and then tell them to go about their normal jobs. The Navy must dedicate itself to PKI and institutionalize the skill sets into rates.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

A. THESIS SUMMARY

The first three chapters of this thesis are designed to provide the reader with the background necessary to comprehend the Navy's DoD PKI implementation strategies outlined in Chapter IV and managing change issues in Chapter V. The results of the research indicate that there are many hurdles the Navy must overcome before it can successfully implement DoD PKI. Ideally, this thesis has provided some new and innovative solutions the Navy can utilize in its implementation of DoD PKI and highlighted some areas the Navy should focus on in order to realize a smooth transition, as a result of the imposed change.

B. THE TRANSITION

The results of this thesis bring the reader to a new set of questions.

- What should the reader do now?
- Where should the Navy focus its resources, i.e., money and people?
- Where can the Navy leverage commercial technology and contractors?
- In regards to training, what do the users and the support structure need to know?

The answers to these questions will help the Navy transition from its current position on implementation of DoD PKI to this thesis' proposed position. The best organization for these comments will be in reference to the three primary research questions.

1. Primary Research Question One

The first primary research question asks how should the Navy organize its public key infrastructure in order to most efficiently and cost effectively implement DoD PKI? The answer to this question is in Chapter IV, but how does the Navy achieve this?

a. PPBS

Funding is going to be one of the deciding factors if DoD PKI makes it in the long run. As soon as possible, the Navy needs to focus its energies on getting a wedge in the POM for current years and establish a firm budget for the out years. The budget needs to address the Navy's hardware needs, i.e., smart cards, smart card readers, finger print scanners, etc. In addition to the user and LRA hardware the Navy needs to address its PKI hardware architecture needs, i.e., directory servers, certificate servers, CRL servers, etc. The architecture of NMCI needs to be budgeted for as well. In addition to hardware, the Navy needs to budget for education. And DoD or the Navy needs to budget for software development. What this all amounts to is an across the board requirements analysis and then a budget submission based thereon.

b. Software Development

Software is the mechanism that is going to truly make this system work. Software development energies and monies need to shift from the current DoD architecture to the one proposed in Chapter IV. A lot of the software functionality might already be available via COTS from industry PKI vendors or from DMDC (i.e., biometrics collection and ID verification). The software needs to address the following areas:

- Centralized Key Escrow

- Decentralized Key Recovery
- Public Key Directories
- Remote Subscriber Identification
- Decentralized Certificate Issuance
- Centralized CRL Maintenance

All of these areas are potential "show stoppers" for DoD PKI and the Navy's implementation of it. Much of the software development will probably be outsourced. Therefore, it is important that DoD pick a software development organization with an excellent reputation for quality, service, and longevity.

c. Standards

The Navy, but more specifically DoD, needs to create a team of professionals to act as its liaison with or lobby for the various standards bodies. It is imperative that DoD gets involved in the standards process as quickly as possible. In many cases, a universally accepted standard is the only thing preventing the DoD or Navy from moving forward. DoD does not want to get ahead of the standards issues and be stuck in a Beta country operating in a VHS world. The Navy's most urgent need is for a standard's based smart card and smart card reader. This would enable them to start the transition form the current DoD ID card to a smart card based DoD ID card.

d. Customer Service

This area is not so easily addressed. The best answer is for the Navy and DoD to change its paradigm regarding customer service. The paradigm that needs to be installed is that of unified support. All the Sailors in the Navy and all the uniformed services are a team. They all work toward the same goal of supporting the operational

forces, specifically the Unified Commands. Having said this, this may be too cultural of an issue to fix short term and outsourcing may be the answer. Industry seems to understand the importance of customer service better than DoD anyway; then again their bottom line is based on dollars and cents.

e. Education

Education will be the spark that will start the PKI fire. The applications that utilize DoD PKI will be the fuel. Educating the masses is the first step to Navy wide acceptance of DoD PKI. The Navy needs to start marketing the idea of IA and how PKI will improve it. They need to devise an aggressive advertising campaign aimed at simply educating every Sailor about the significance of DoD PKI and what it can do for them. This can start with command meetings and then migrate to online tutorials. These tutorials should be "cool" so the young Sailor will enjoy learning the processes that support PKI. Mobile training teams need to educate the LRAs and the RITSC operators. All or most of these functions can be outsourced. The commercial industry has been successfully providing this type of training to civilian companies for years. They should be leveraged, at least in the near term, for their expertise and immediate usability.

2. Primary Research Question Two

The second primary research question deals with how will the Navy distribute key pairs to 365,108 active duty, 196,986 ready reserve, and 195,058 civilian personnel [Ref. 5]. The answer to this question is in Chapter IV, but how will the Navy do this?

a. Implementation Strategy

The answer lies in their implementation plan. If the Navy follows the path proposed in this thesis, then an investment in technology must be made; this is addressed

above. However, certain other issues must be addressed as well. First, a partnership with DMDC must be established. Based on the author's interview with the Deputy Director of DMDC, DMDC could take on the additional responsibilities outlined in Chapter IV [Ref. 13]. DMDC would have to adjust its databases, but this is easily done. The major problem would be in populating the databases [Ref. 13]. Therefore, a plan of attack needs to be formulated that will ensure all civilian employees, uniformed service members, and DoD foreign nationals were added to the database and their personal and biometrics information captured and stored. This could be done with the current infrastructure of DEERS/RAPIDS centers.

If on the other hand the current DoD implementation plan continues, then a close partnership with industry must be initiated. The process of distributing keys needs to be outsourced to the greatest extent possible. It will be an extremely labor intensive process with a steep learning curve that is best managed with contractors. There is no value added to the process by pulling LRAs from across the Navy to go on a travelling "road show". It would be expensive and the service members would be away from their commands for quite some time.

b. Policy

Certain policies need to be modified before the Navy can implement the ideas contained in this thesis. To that end, the Navy's first order of business is to address the policy-making authorities with the enclosed proposed changes, specifically the requirement for in-person identity verification. Without DoD's movement on this issue, much of the value contained herein is lost. The author feels the Navy could get a policy change if it presents a well thought out and "executable" plan. In addition, policy

concerning the capturing of civilian and foreign national biometrics needs to addressed. This could end up being a political issue, i.e., personal liberties. The DoD can easily handle this by making it a requirement for employment. Policy concerning which hardware will be PKI enabled needs to be addressed too. The Navy's architecture will continue to be vulnerable to outsiders if only servers are PKI enabled. CNO N6 and his staff appear to be the appropriate group to address these policy issues, but it may take DON CIO to make this happen.

3. Primary Research Question Three

The third primary research question deals with how the Navy will manage the change-related issues surrounding the implementation of DoD PKI? The answer to this question is in Chapter V, but how will the Navy do this?

The Navy needs two things early on to address this issue, strong leadership and education. Education was addressed above, but one more reference is appropriate. If the masses do not feel the need for PKI, it will fail, at least in the universal acceptance sense. To address this, the Navy needs to develop PKI aware applications that Sailors care about and need. If PKI improves the quality of life for Sailors, it will be a huge success. Therefore, education to PKI's capabilities must be made early and often. Every Sailor must know what PKI means and is, long before he is handed a smart card. A large driver in this education is the Navy's leadership.

DON CIO and CNO (N6) need to be the Navy's strong advocates for PKI. They need to be visible and vocal. DON CIO needs to craft the Department of the Navy's vision for PKI. In turn, CNO (N6) needs to take this vision and craft the Navy's vision for PKI. As soon as it is practical this vision needs to reach every Sailor in the Navy.

Once this occurs, CNO (N6) needs to adopt disciples to his vision. Then he and his disciples need to address the Navy and their concerns surrounding PKI. They should elicit support for the cause and continue to set the example for the rest of the Navy to follow. They should not mandate support, but rather foster it through a strong vision, a sound infrastructure, and useable applications.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

During the course of the author's research, many collateral issues surrounding DoD PKI, its implementation, and organizational responses to it were uncovered. The importance of DoD PKI can not be overemphasized and any continued study in this area would be extremely beneficial to the U.S. military and national defense. Areas for future research:

- An analysis of relationship between the DoD CIO, DON CIO, CMC (C4I), and CNO (N6) and how information management is perceived and handled.
- An analysis of the interactivity bandwidth requirements of PKI and how network connectivity is affected as a result of its implementation.
- Development of a model to test the feasibility of utilizing DoD PKI on the battlefield in a wireless environment.
- Extending the idea of a tactical PKI, strategies for rapid revocation of certificates and accessing of escrowed keys needs to be developed, i.e., when service member and or smart card are captured.
- A before and after implementation study of NMCI and how it enhances information security in the Navy.

- A study into the advantages and disadvantages surrounding DMDC involvement in DoD PKI.
- Establishment of metrics for PKI.

LIST OF REFERENCES

1. Comer, Douglas E., *Computer Networks and Internets*, Prentice Hall, 1997.

2. White, Gregory B., Fisch, Eric A., and Pooch, Udo W., *Computer System and Network Security*, CRC Press LLC, 1996.

3. Campbell, Roy, "CS423 Lecture Notes." [http://www-courses.cs.uiuc.edu/~cs423/lectures/old13/img036.htm]. April 7, 1998.

4. Verton, Daniel, "New Battle Lines Being Drawn Over Encryption Debate." [http://www.idg.net/new_docids/new_docid_9-128410.html]. April 14, 1999.

5. MITRE/DISA/NSA, *DoD Information Infrastructure Public Key Infrastructure (PKI) Concept of Operations*, October 24, 1997.

6. DISA/NSA, *Public Key Infrastructure Roadmap for the Department of Defense*, June 14, 1999.

7. Grant, Gail L., *Understanding Digital Signatures – Establishing Trust over the Internet and Other Networks*, McGraw-Hill Companies, Inc., 1998.

8. Telephone conversation between Mr. Jim Brandt, Verisign and the author, April 29, 1999.

9. United States Department of Defense, *X.509 Certificate Policy*, Version 2.0, March 1999.

10. United States Department of Defense, *Certification Practice Statement for the Certificate Management Infrastructure of the Defense Information Infrastructure*, Version 2.0, April 10, 1998.

11. Deputy Secretary of Defense Memorandum to Secretaries of the Military Departments, and others, Subject: Department of Defense (DoD) Public Key Infrastructure (PKI), May 6, 1999.

12. Information Technology Infrastructure (ITI) Integrated Product Team (IPT), *Department of the Navy Information Technology Infrastructure Architecture*, Version 1.0, March 16, 1999.

13. Brandewie, Robert, *DEERS & RAPIDS Systems Presentation*, DON CIO PKI Implementation Conference, June 29, 1999.

14. Cieri, Tony, *DON Smart Card Status Report*, DON CIO PKI Implementation Conference, June 29, 1999.

15. Wendling, CAPT Mike, *PKI Funding Status*, DON CIO PKI Implementation Conference, June 29, 1999.

16. Wright, Capt Carl, USMC DoD PKI Implementation Conference, June 8, 1999.

17. Jick, Todd D., *Managing Change*, The McGraw-Hill Companies, Inc., 1993.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dryer Rd.
   Monterey, CA 93943-5101

3. Director, Training and Education 1
   MCCDC, Code C46
   1019 Elliot Rd.
   Quantico, VA 22134-5027

4. Director, Marine Corps Research Center 2
   MCCDC, Code C40RC
   2040 Broadway Street
   Quantico, VA 22134-5107

5. Director, Studies and Analysis Division 1
   MCCDC, Code C45
   300 Russell Road
   Quantico, VA 22134-5130

6. Professor Rex Buddenberg (Code IT/Bu) 1
   Naval Postgraduate School
   Monterey, CA 93943-5002

7. Professor John Osmundson (Code CC/Os) 1
   Naval Postgraduate School
   Monterey, CA 93943-5002

8. Professor Dan Boger (Code IT/Bo) 1
   Naval Postgraduate School
   Monterey, CA 93943-5002

9. Deputy Director, Defense Manpower Data Center 1
   DoD Center Monterey Bay
   400 Gigling Road
   Seaside, CA 93955-6771

10. DON CIO 1
1000 Navy Pentagon
Washington, DC 20350-1000

11. Major Christopher J. Michelsen 3
Marine Corps Systems Command
2033 Barnett Avenue, Suite 315
Quantico, VA 2134-5010