



Design and development of a web-based DOD PKI common access card (CAC) instruction tool

Title	Design and development of a web-based DOD PKI common access card (CAC) instruction tool
Item Type	Thesis
Authors	Athanasopoulos, Vasileios D.
URI	https://hdl.handle.net/10945/1714
Publisher	Monterey, CA; Naval Postgraduate School
Date Issued	2004-03
Rights	Copyright is reserved by the copyright owner.
Download date	2026-04-14 11:14:21
Link to Item	https://hdl.handle.net/10945/1714

Downloaded from NPS Archive: Calhoun



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**DESIGN AND DEVELOPMENT OF A WEB-BASED
DOD PKI COMMON ACCESS CARD (CAC)
INSTRUCTION TOOL**

by

Vasileios Athanasopoulos

March 2004

Thesis Co-Advisors:

Cynthia E. Irvine

J. D. Fulp

Second Reader:

Glenn R. Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
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 March 2004	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Design and Development of a Web-Based DOD PKI Common Access Card (CAC) Instruction Tool			5. FUNDING NUMBERS
6. AUTHOR(S) Vasileios Athanasopoulos			8. PERFORMING ORGANIZATION REPORT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			10. SPONSORING/MONITORING AGENCY REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			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) Public key cryptography and the infrastructure that has been designed to successfully implement it: Public Key Infrastructure (PKI) is a very promising computer security technology. As a significant enhancement to this infrastructure, the DoD is now issuing smart card tokens, in the form of the Common Access Card (CAC), to its service members. This card is a relatively complex cryptographic device that contains its user's private keys, digital certificates, and other personal/administrative information. Service personnel are being issued these cards with little or no training regarding what they are or how they function. Such an omission detracts from the infrastructure's overall security. This thesis presents an introductory-level description of public key cryptography and its supporting infrastructure (PKI). The thesis then goes on to develop a web-based training tool that could provide all DoD CAC holders with the rudimentary knowledge of how their CAC fits into the broader infrastructure. The training tool will require no instructor, and will present a validation test to each user. DoD commands could utilize this tool to provide basic CAC training to their members.			
14. SUBJECT TERMS Cryptography, Symmetric Cryptography, Asymmetric Cryptography, Public Key, Private Key, Public Key Infrastructure (PKI), DoD PKI, Certificate, Certificate Authority (CA), Local Registration Authority (LRA), Common Access Card (CAC), Web-Based Tutorial.			15. NUMBER OF PAGES 100
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**DESIGN AND DEVELOPMENT OF A WEB-BASED DOD PKI COMMON
ACCESS CARD (CAC) INSTRUCTION TOOL**

Vasileios D. Athanasopoulos
Lieutenant Commander, Hellenic Navy
B.S., Hellenic Naval Academy, 1990

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN COMPUTER SCIENCE
and
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2004**

Author: Vasileios Athanasopoulos

Approved by: Cynthia E. Irvine
Thesis Co-Advisor

J. D. Fulp
Thesis Co-Advisor

Glenn R. Cook
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Public key cryptography and the infrastructure that has been designed to successfully implement it, the Public Key Infrastructure (PKI), is a very promising computer security technology. As a significant enhancement to this infrastructure, DoD is now issuing smart card tokens, in the form of the Common Access Card (CAC), to its service members. This card is a relatively complex cryptographic device that contains its user's private keys, digital certificates, and other personal/administrative information. Service personnel are being issued these cards with little or no training regarding what they are or how they function. Such an omission detracts from the infrastructure's overall security.

This thesis presents an introductory-level description of public key cryptography and its supporting infrastructure (PKI). The thesis then goes on to develop a web-based training tool that could provide all DoD CAC holders with the rudimentary knowledge of how their CAC fits into the broader infrastructure. The training tool will require no instructor, and will present a validation test to each user. DoD commands could utilize this tool to provide basic CAC training to their members.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	TRAINING FRAMEWORK	2
C.	AREA OF RESEARCH AND RESEARCH OBJECTIVES	3
D.	SCOPE AND ASSUMPTIONS.....	3
E.	RESEARCH QUESTIONS.....	4
F.	ORGANIZATION OF THESIS	4
II.	ASYMMETRIC CRYPTOGRAPHY	7
A.	GENERAL OVERVIEW	7
B.	HOW IT WORKS.....	9
III.	OVERVIEW OF PKI	19
A.	WHAT IS A PUBLIC KEY INFRASTRUCTURE (PKI)?	19
B.	WHAT CAN YOU DO WITH A PKI?	20
C.	CERTIFICATES.....	22
1.	Identity	22
2.	E-Mail Signature.....	23
3.	E-Mail Encryption	23
4.	Server	23
D.	MAJOR COMPONENTS	23
1.	Certificate Authority (CA).....	24
2.	Registration Authority (RA)	25
3.	Local Registration Authority (LRA).....	25
4.	Directory (or Repository).....	26
5.	Users	26
E.	CERTIFICATE REVOCATION LISTS.....	27
IV.	THE COMMON ACCESS CARD	31
A.	INTRODUCTION.....	31
B.	BACKGROUND	32
C.	CONTENT.....	33
D.	DOD AND THE COMMON ACCESS CARD (CAC)	35
1.	Benefits of the CAC	35
2.	Common Access Card's Design	36
3.	CAC Functionality	37
V.	TRAINING FOR THE DOD PKI	41
A.	THE TRAINING NEED.....	41
B.	CURRENT TRAINING STATUS.....	42
C.	A DOD PKI AND CAC INSTRUCTION TOOL	43
1.	Why Web-Based Training.....	43
2.	PKI and CAC Instruction Tool General Overview	45
D.	INSTRUCTION TOOL DESIGN AND DEVELOPMENT	46

1.	Goals and Required Functionality	46
2.	Tutorial's Design.....	47
3.	Web Site Hierarchy.....	47
4.	Tutorial's Database Sketch	51
5.	Tutorial's Maintenance and Control	51
6.	Tracking the Training	52
VI.	CONCLUSIONS AND FUTURE WORK.....	53
A.	CONCLUSIONS	53
B.	FUTURE WORK.....	55
	APPENDIX. INSTRUCTION TOOL SCREENSHOTS	57
	LIST OF REFERENCES.....	77
	BIBLIOGRAPHY.....	79
	INITIAL DISTRIBUTION LIST	81

LIST OF FIGURES

Figure 1.	Public/Private Key Pair [From: 1, Slide 38]	7
Figure 2.	Public Key Used for Encryption [From: 4, Slide 19]	9
Figure 3.	Asymmetric Encryption (Confidentiality) [From: 5].....	11
Figure 4.	Digital Signature Creation [From: 4, Slide 20].....	13
Figure 5.	Digital Signature Verification [From: 4, Slide 20]	14
Figure 6.	Digital Signing (Authentication, Integrity, Non-Repudiation) [From: 5, p. 9]	14
Figure 7.	Digital Certificate [From: 1, Slide 21]	17
Figure 8.	Figure Certificate Fields [From: 1, Slide 22].....	22
Figure 9.	DoD PKI (Hierarchical) Trust Model [From: 10, Slide 11]	24
Figure 10.	User Registration [From: 1, Slide 33].....	27
Figure 11.	CAC Front View [From: 11, Slide 11]	34
Figure 12.	CAC Rear View [From: 11, Slide 12]	34
Figure 13.	CAC View. [From: 13, Slide 2].....	35
Figure 14.	Chip Allocation [From: 14, p. 1]	37
Figure 15.	CAC Card's Key Pairs	39
Figure 16.	Digital Signature and Encryption [From: 11, Slide 15].....	40
Figure 17.	DoD PKI and CAC Tutorial's General Diagram	49
Figure 18.	Login Screen	57
Figure 19.	Home Page	58
Figure 20.	Lectures Contents.....	59
Figure 21.	Secret Key Cryptography Introduction.....	60
Figure 22.	Public Key Cryptography Introduction.....	61
Figure 23.	Public Key Cryptography (cont.).....	62
Figure 24.	Digital Signature	63
Figure 25.	Certificates	64
Figure 26.	Types of Certificates	65
Figure 27.	Certification Authority.....	66
Figure 28.	Certificate Verification	67
Figure 29.	Certificate Revocation List (CRL).....	68
Figure 30.	Introduction to Public Key Infrastructure	69
Figure 31.	PKI Components.....	70
Figure 32.	CAC Introduction.....	71
Figure 33.	Common Access Card (CAC).....	72
Figure 34.	Common Access Card's Design	73
Figure 35.	Common Access Card & DoD.....	74
Figure 36.	CAC and PKI	75
Figure 37.	Test Page.....	76

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Public/Private Keys Usage [From: 7]	15
Table 2.	PKI Security Services [From: 10, Slide 8].....	21
Table 3.	Certificates Usage [From: 11, Slide 8]	23
Table 4.	DoD PKI and CAC Tutorial Pages	50

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

After spending almost three years of my life in the United States I feel happy that I have finished my studies, but I have to admit that many people participated in this effort.

First, I would like to thank my thesis advisor J. D. Fulp for his high level of professionalism and guidance and my co-advisor, Professor Cynthia Irvine, and second reader, Mr. Glenn Cook, for their support.

Next, I would like to dedicate this achievement to my parents for their continuous support, especially during some difficult moments. Specifically, I would like to acknowledge: My father, Dimos Athanasopoulos, for his encouragement to this effort and generally, for his advices concerning my naval career, and my mother, Katina Athanasopoulou, for her endless love, support and understanding.

Additionally, I would like to thank the Hellenic Navy for giving me this chance and the promise of many more experiences.

Finally, I want to say that during my stay here, I was lucky enough to make some new friendships. I will never forget this period of my life and it will always be on my mind and in my heart as a lighthouse, which showed me the road to better discover and improve myself and provided me with a deeper understanding of life and human relationships.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Living in the today's Internet era has made it more obvious that security requirements have necessarily increased, especially within large organizations such as Department of Defense (DoD). In order to meet these requirements, the DoD decided to develop and implement a Public Key Infrastructure (PKI) as a way of securing information that is exchanged across either its own networks, or the public Internet. This thesis attempts to provide a basic overview of public (also know as "asymmetric") key cryptography, the infrastructure that is designed to support it (i.e., the Public Key Infrastructure, or PKI), and finally; the design, merits, and usage of the DoD Common Access Card (CAC) and how it fits within the infrastructure to enhance its security.

It is obvious that with all the changes taking place within the DoD environment regarding the incorporation of new procedures and technologies to enhance security, some problems are arising. The successful implementation of this effort will be based on the workforce's adoption of the new technologies. Therefore, the basic requirement is to enhance personnel training and awareness. The workforce must understand how the infrastructure works, what their role is in it, what the consequences of their actions are, and how their organizational behavior can affect its successful implementation.

From all the above, we can easily see that the role of user training is essential for the successful implementation of the DoD's PKI. The main scope of this training must be to provide users with knowledge that will help them to reduce or eliminate any mistakes that could threaten the infrastructure's trustworthiness and integrity.

A. PROBLEM STATEMENT

The PKI training provided to DoD personnel is rather problematic. These problems result because existing training was developed under the purview of different commands among the different services; that is, there is not a centrally controlled authority that dictates a training standard. Consequently, DoD personnel might not have the same knowledge and understanding of the entire PKI environment.

Besides the difficulties in understanding the PKI technology, the relatively recent introduction and use of the Common Access Card (CAC) has made this problem even more complex, and thus the user's need for training even more necessary than before.

There is a need for a more centrally provided and managed training resource for DoD users. This resource needs to provide DoD personnel an overview tutorial of the operation of the DoD Public Key Infrastructure (PKI) and particularly, the role of the Common Access Card (CAC) in the infrastructure. This solution can leverage Web development and delivery techniques to provide a more user-friendly experience.

B. TRAINING FRAMEWORK

The well-known adage that the overall strength of a chain is limited by the strength of its weakest link is equally applicable to most composite security technology, of which a PKI implementation is a good example. Given that PKI is a fairly new and not widely understood security technology, user misunderstanding and the consequent errors may likely become the “weakest link” of the infrastructure. Much literature¹ exists indicating the importance of well-educated and trained people for the successful implementation of a PKI.

This thesis will examine the training needs, and develop a DoD PKI training tool with emphasis on the design and development of an online instruction tutorial for users of the Common Access Card (CAC). The thesis will present a basic overview of PKI and smart card technologies, starting with a short presentation of the existing training situation in order to show the difficulties that exist and the consequent misunderstandings that can result. This thesis will be follow-on work to Marcia L. Ziemba's thesis², which was a great help in my effort.

¹ “...it may be beneficial to institute internal training programs...to help educate the appropriate personnel” (p. 269). This section indicates the need for training when implementing a PKI. [Adams, C. and Lloyd, S., Understanding Public-Key Infrastructure – Concepts, Standards, and Deployment Considerations, Macmillan Technical Publishing, Indianapolis, Indiana, 1999].

² Marcia L. Ziemba, “A training framework for the department of defense public key infrastructure”, Master's Thesis Naval Postgraduate School, Monterey, California, September 2001.

The final product of this thesis will be a Web-based training tool that will present the basic subject material required for the DoD CAC users to employ their cards properly. This thesis should contribute to DoD's training requirements and help it maintain its required levels of security.

C. AREA OF RESEARCH AND RESEARCH OBJECTIVES

To conduct this research, the following steps were required:

- Examine research papers and literature on PKI technology (textbook, online resources, DoD documents, and other electronic reference services).
- Conduct specific searches for any existing DoD PKI CAC user training tools.
- Obtain and utilize a CAC for personal experience and exposure.
- Determine and summarize the larger PKI environment and the essential knowledge elements for the general CAC user that will subsequently be formatted for the Web-based tutorial.
- Select and create a bank of appropriate test/evaluation questions.
- Implement test evaluation functionality into the Web-based tutorial.
- Ensure that the test evaluation functionality can provide a pass or fail message to an appropriately configured database server.

D. SCOPE AND ASSUMPTIONS

The intent of this work is to produce a tool that provides relevant subject matter education on the design, use, and ownership of a DoD PKI Common Access Card (CAC).

The education provided by this tool should meet the following requirements by being:

- Targeted to the general CAC user (vice higher level PKI authorities),
- Formatted for Web-based delivery/access,
- Pedagogically sufficient as a self-tutoring tool (no instructor necessary), and
- Provide a built-in question bank with test and evaluation functionality.

E. RESEARCH QUESTIONS

The questions that this thesis will address are the following:

Primary research question: What is the most pertinent content, organization, and format for the delivery of a DoD PKI Common Access Card (CAC) online education tool?

Other subsidiary research questions that this thesis will try to answer are:

- What are the essential elements of DoD PKI of which all DoD CAC card users should be knowledgeable?
- What similar educational tools may already exist and if yes, do they sufficiently satisfy the requirements set forth herein?
- How should the essential DoD CAC card user knowledge elements be organized for an online self-tutorial education experience?
- What software development tools (e.g., Java Applets, FrontPage, XML, etc.) should be used to create the most interesting and didactically efficient learning experience?
- How should the tool's screen display be organized to provide simple and intuitive navigation within the learning tool?
- What is the appropriate pool of subject matter test questions from which a pass or fail determination can be made?
- How should tests be generated from the test question pool to guarantee that all knowledge elements are tested sufficiently?

F. ORGANIZATION OF THESIS

The organization of this thesis includes the following chapters and appendices.

Chapter I: Introduction – This chapter introduces the concept of the DoD PKI and recognizes the need for proper personnel training.

Chapter II: Public Key Cryptography – This chapter offers a basic synopsis of Secret (symmetric) key and Public (asymmetric) key cryptography theories along with some description of their use.

Chapter III: Public Key Infrastructure (PKI) – This chapter sketches the concept of a Public Key Infrastructure (PKI) along with some of its implementation details.

Chapter IV: Common Access Card (CAC) – This chapter provides a general outline of the Common Access Card (CAC) and describes its use within the DoD PKI.

Chapter V: PKI Training within DoD – This chapter presents the current situation and argues for a change in the training methods, through the adoption of web-based training.

Chapter VI: Conclusion and Future Work – This chapter reviews the main concepts and findings of this thesis, and presents some related topics for future research, which might prove useful for the improvement of the training tool developed herein.

Appendix: Instruction Tool Design – This chapter presents a basic overview of the DoD PKI and Common Access Card (CAC) Training instruction tool design. This is a presentation of screen shots from the DoD PKI and Common Access Card (CAC) training instruction tool.

THIS PAGE INTENTIONALLY LEFT BLANK

II. ASYMMETRIC CRYPTOGRAPHY

Symmetric key cryptography raises some problems related to its implementation. These problems are associated with the authenticity of information processed with a symmetric key, and with the secure distribution of the key among users. With simple implementations of symmetric key cryptography, a recipient will not know for sure who the originator of the encrypted message is because anyone in possession of the key could have been the sender.

A solution to these problems was provided with the introduction of asymmetric (public) key cryptography. Its basic principle is very different from the single encrypt/decrypt key of symmetric key cryptography, in that every user owns a key pair: one key called the *public key* and the other called the *private key*. Although implementing a system that uses asymmetric public key cryptography adds complexity, the benefits gained are very appealing.

A. GENERAL OVERVIEW

Asymmetric cryptography, also known as public key cryptography, in general, provides the same services as Symmetric Key Cryptography, but it uses different keys for encryption and decryption. Public key technology is based on key pairs. A key pair in a public key cryptography scheme consists of a private key and a public key.

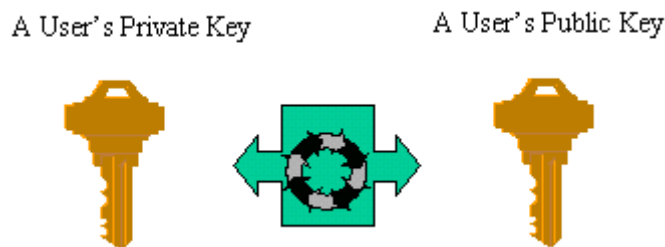


Figure 1. Public/Private Key Pair [From: 1, Slide 38]

The basic characteristics of the public and private keys are:

- A key is a binary string.
- The public and private keys are generated at the same time by a special software program.
- The keys are not identical, but have a unique relationship so that they will only work with each other to encrypt and decrypt information. These key pairs are generated by a process that ensures the keys are uniquely paired with one another and that neither key can be determined from an inspection of the other. [2]
- Information encrypted with one key can only be decrypted by the other, and vice-versa. In other words, a message encrypted using the public key, can only be decrypted by that key's corresponding private key.
- Each entity in a public key system will be assigned a mathematically related private and public key pair. [3]
- The private key is
 - Protected by the owner,
 - Used to digitally sign messages,
 - Used to decrypt messages, and
 - Kept in the physical and/or cryptographic protection of the owner
- The public key is
 - Distributed freely and is accessible to anyone,
 - Used to verify digital signatures,
 - Used to encrypt messages, and
 - Stored inside of "digital certificates" that provide for the integrity and authenticity of the user to public key value binding.
- Though public keys can be distributed freely, once they have been enclosed within their protective certificates, private keys should never leave the possession of their owners (a policy exception to this rule is discussed later under the topic "key escrow")

Public key cryptography is, therefore used, for the encryption/decryption and signing/verification of information. Encrypting information ensures privacy by preventing unintended disclosure, and signing messages authenticates the sender of the message and ensures the message has not been modified since it was sent.

B. HOW IT WORKS

With the use of public key cryptography, when anyone wants to send information to another, that person only has to obtain a copy of that other person's public key and encrypt the message to be sent using that key.

Although the preceding paragraph provides a cursory description of asymmetric cryptography being used to ensure confidentiality, the following material will elaborate on the details.

Figure 2 shows the process of sending a message using a public key system.

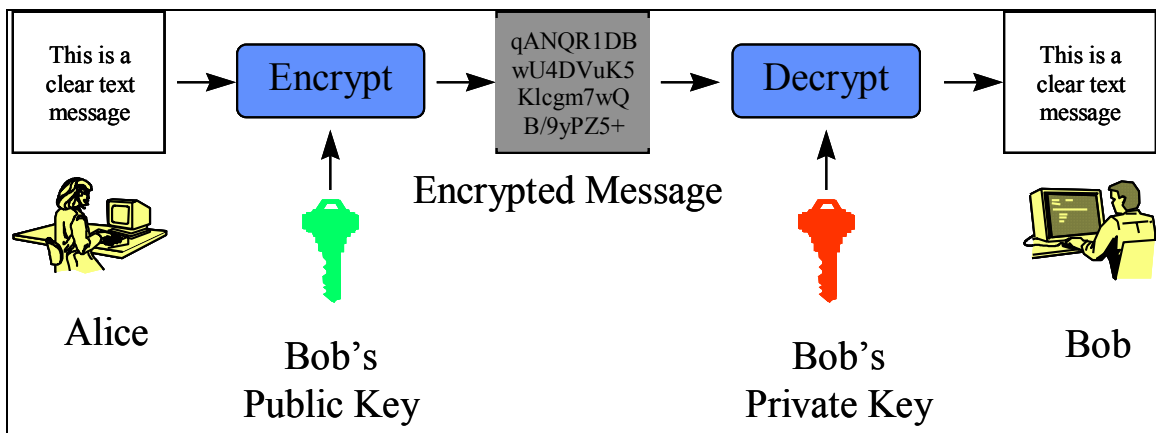


Figure 2. Public Key Used for Encryption [From: 4, Slide 19]

Alice wants to send a message to Bob so that Bob is the only one who can read the message (confidentiality). So:

- Alice obtains Bob's public key.
- Alice encrypts the message with Bob's public key.
- Alice sends the encrypted message to Bob.
- Bob uses his private key to decrypt the message.

The aforementioned information implies that Bob is the only one who will be able to decrypt this message since he is the only one who possesses his (Bob's) private key. If the message is intercepted during transmission, the interceptor will not be able to decrypt it.

Therefore, in this scheme, the keys are used as follows:

- The Public Key is used for encryption

The sender uses the recipient's public key when desiring to send confidential information. The information to be sent is encrypted using the recipient's public key. The recipient can send the public key to the sender, or the sender can retrieve it from the directory in which it is published.

- The Private Key is used for decryption

A private key is used to decrypt information that has been encrypted using its corresponding public key. Both the sender and receiver of a message that has been encrypted with the receiver's public key, can be sure that only the receiver can decrypt the message. The receiver; however, cannot be sure of the message's sender, as it is possible for anyone to have the public key used to encrypt it.

In normal practice, both symmetric and asymmetric cryptographic mechanisms are used together in order to take advantage of the strengths of each; specifically, the ability to distribute public keys without concerns of confidentiality (a strength of asymmetric key cryptography), and the faster encryption/decryption speed of secret keys (a strength of symmetric key cryptography relative to asymmetric). The general usage, therefore, is to use an asymmetric mechanism to deliver a secret key securely, then to have the actual information being sent encrypted using the secret key. This secret key can be any sufficiently long random number. Since the general usage is to generate at least one new secret key for each session of communication between two parties, the secret key is often also referred to as the session key. The public key is used to encrypt the session key and both the session key and the information encrypted with it are sent to the recipient. The recipient will use the private key to decrypt the session key, and then use the session key to decrypt the actual information. This is much faster than using the private key to decrypt all of the information. Figure 3 illustrates this practice.

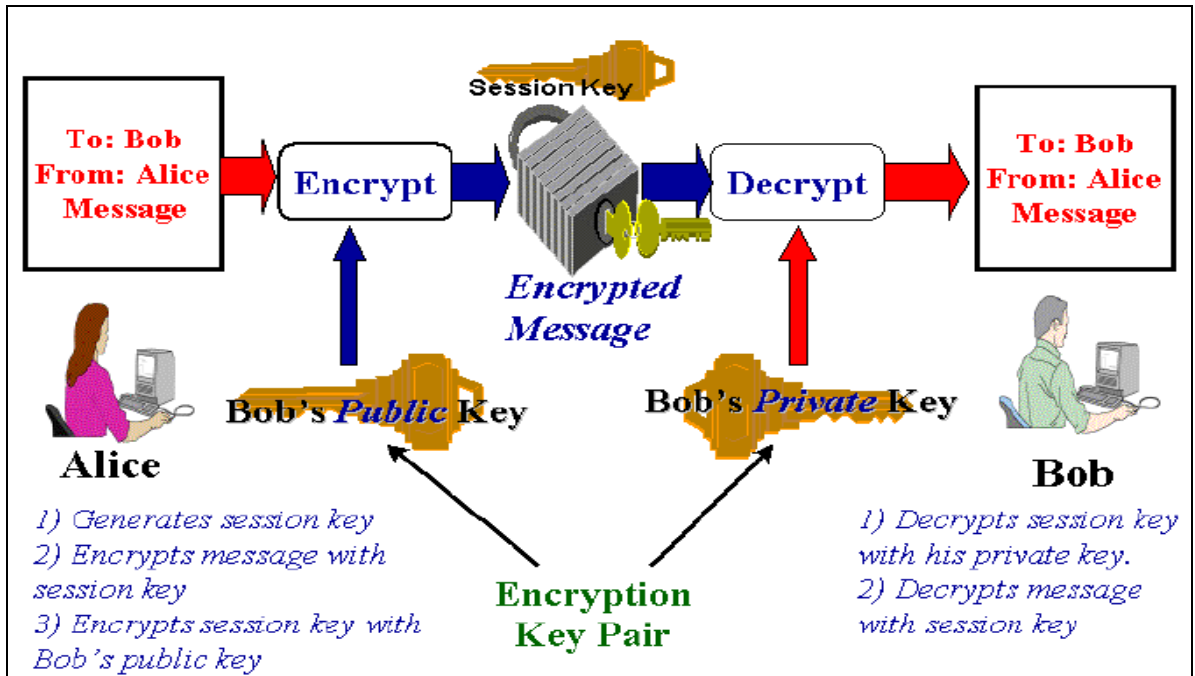


Figure 3. Asymmetric Encryption (Confidentiality) [From: 5]

- Alice encrypts the message with the symmetric key
- Alice encrypts the symmetric key with Bob's public key.
- Alice sends both the encrypted message and the encrypted symmetric key to Bob.
- Bob uses his private key to decrypt the encrypted symmetric key.
- Bob uses the symmetric key to decrypt the encrypted message.

However, a problem still exists. Although confidentiality has been achieved because only the intended recipient of the message was able to decrypt it, there is no proof regarding from whom the message came, since anyone could have used the recipient's public key to encrypt the message.

It is under these circumstances that the concept/mechanism of a *digital signature* comes into good use. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been signed is unchanged.

A digital signature can be used on any binary string. Unlike a hand-written signature which is slightly different every time it is made, digital signatures are mathematically precise and reproducible. A further benefit of digital signatures is that timestamps can be included in the signed material thus establishing a means of recording the time that a signature was applied. Since digital signing is mathematically applied “over” the entire signed binary string which comprises the document, the document cannot feasibly be changed without detection by the signature verification process. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. Digital signatures provide for authentication, non-repudiation, and integrity of the information to which they are applied.

Digital signatures must not be confused with a *digital certificate*: which is a kind of electronic container for a user’s public key which has been digitally signed by the certificate-issuing authority to certify its validity.

The recipient of a digitally signed message, having the public key of the signer, can determine:

- if the message was created with the signer’s private key, and
- if the message was altered since it was signed [6]

When using a digital signature, the data itself is not encrypted, but a hash of the data is encrypted with a private key. A hash (also known as a digest) is a unique, fixed-length mathematical value that is determined by the content of the message and the ‘hashing’ algorithm used to create it. When some specific data is hashed, and the resultant hash value is encrypted with a user’s private key, the result is a digital signature for that specific data. The original data cannot be recovered from its hash, thereby resulting in the use of the term “one-way hash”.

The “signed” value is either attached to the end of the data or is sent as a separate file together with the data if the data is later transmitted to a remote location. The sender’s public key may also be sent with the message in the form of a certificate. Figure 4 illustrates the creation of a digital signature.

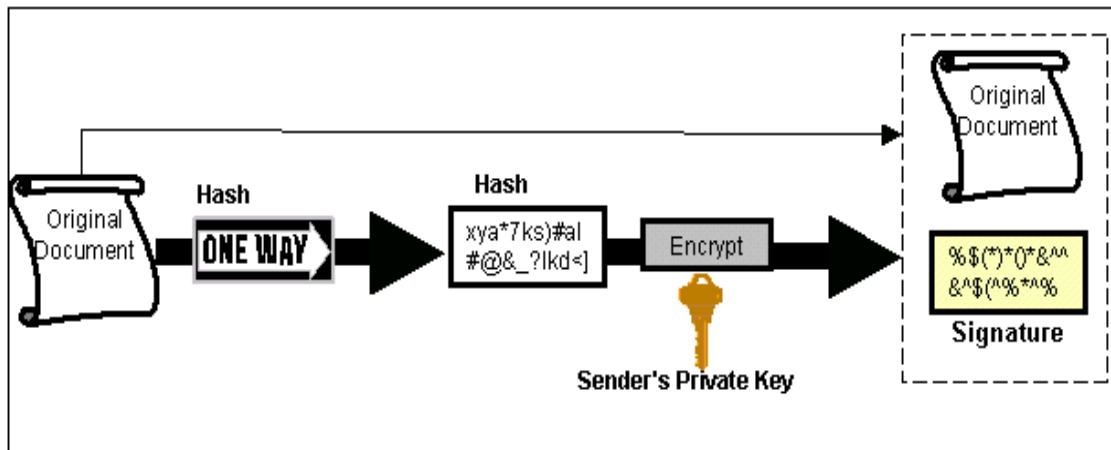


Figure 4. Digital Signature Creation [From: 4, Slide 20]

In order to verify the received data, the recipient of a digitally signed message performs the following steps.

- Uses the public key of the sender to decrypt the latter's digital signature and extract the encrypted hash value that the sender calculated for the information.
- Calculates the hash value for the received data using the same hashing algorithm that the sender used.
- Compares the two hash values, i.e., the newly calculated hash value is compared to the hash value that the sender originally calculated.
 - If the values match, the receiver is certain that the person controlling the private key (corresponding to the public key) sent the data and also knows that the data has not been altered since it was signed.
 - If they do not match, the receiver knows that either the document has changed or the sender is not who he/she claims to be.

If no errors have been found, the receiver can be certain of the authenticity and integrity of the information that has been received. Figure 5 illustrates the verification of a digital signature.

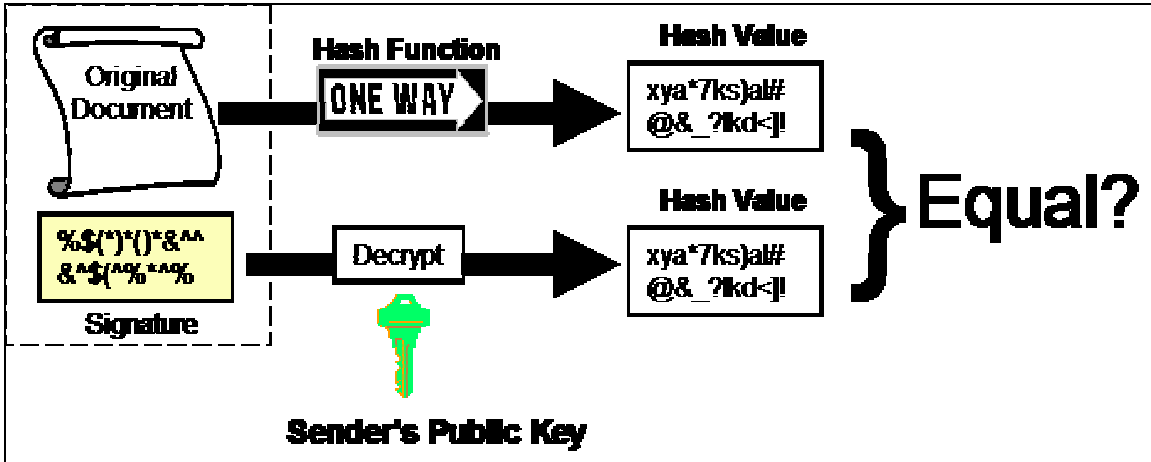


Figure 5. Digital Signature Verification [From: 4, Slide 20]

Figure 6 shows the overall picture of how a digital signature works.

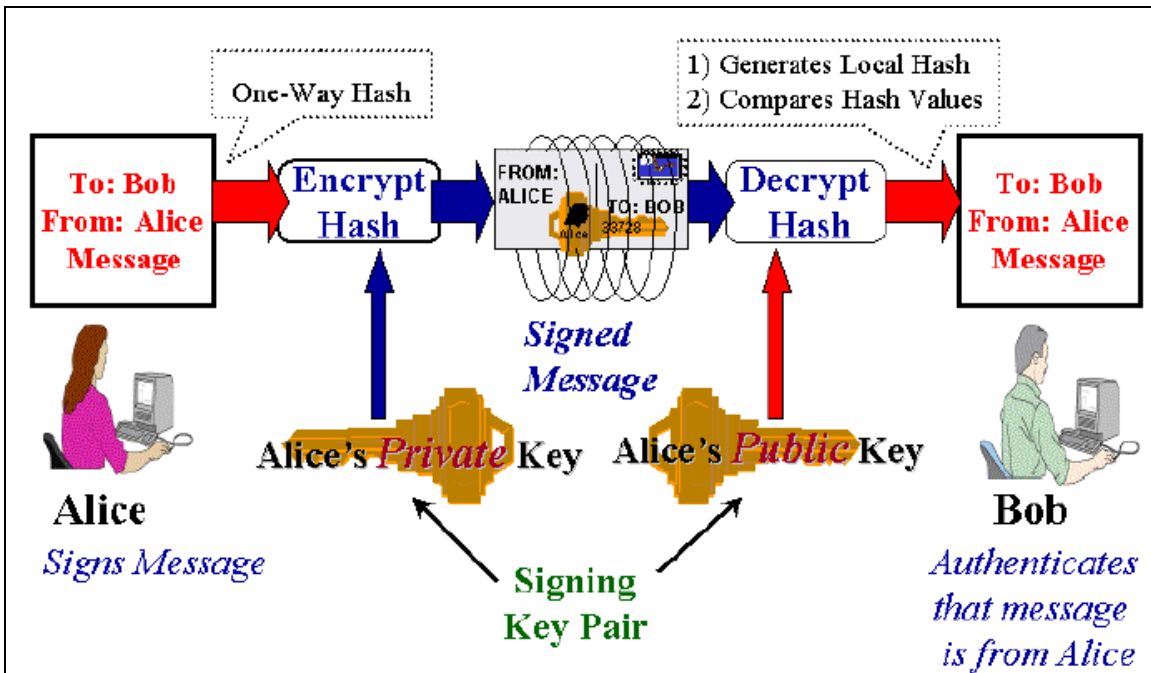


Figure 6. Digital Signing (Authentication, Integrity, Non-Repudiation) [From: 5, p. 9]

Thus, in this scheme the use of keys is:

- The Private Key for Signature

If the sender wishes to prove to a recipient that he or she is the source of the information, the sender uses his or her private key to digitally sign a message (a digital signature).

- The Public Key for Signature

The receiver of a digitally signed message uses the sender's public key to verify the signature so that the receiver knows that the person controlling the private key corresponding to the public key sent the information, and that the received information has not been altered since it was signed.

Table 1 summarizes the uses of public and private keys in asymmetric cryptography:

Key Function	Key Type	Whose Key Used
Encrypt data for a recipient	Public key	Receiver
Sign data	Private key	Sender
Decrypt data received	Private key	Receiver
Verify a signature	Public key	Sender

Table 1. Public/Private Keys Usage [From: 7]

Currently, Public Key encryption and digital signatures are used in order to provide the following services: confidentiality, authenticity, integrity, and non-repudiation.. It therefore ensures that:

- the data has not been altered,
- the data actually came from the stated sender, and
- that only the intended recipient will be able to read the message.

Although use of the techniques described above have solved many problems regarding data integrity and authentication, a big question still remains unanswered: how can the recipient of a digitally signed message be assured of the validity of the certificate that is used to verify the signature? There must be a level of trust within the system in order for public key encryption to be legitimate. A cryptographic binding between a

user's identity (and possibly other credentials) and his/her public key(s) must take place. This binding and required level of trust can be achieved through digital certificates and Certification Authorities within a public key infrastructure.

A *digital certificate* is an electronic “document” or computer generated record that officially links together the subscriber's identification with the corresponding public key. [1, Slide 18] The certificate is digitally signed by the issuing Certification Authority (CA) to ensure the certificate's authenticity so that anyone in possession of the CA's public key can verify the legitimacy of the certificate.

Certificate Authorities (CA's) will provide a requestor with someone's public key contained in a certificate. Information in the certificate will identify the public key's owner, and provide the name of the CA who validated the identity and signed the identity-to-public-key binding. In this way it is possible to see that a certificate serves as a kind of protective “container” for the public key, protecting the integrity of its binding to an owner and authenticating both the binding and identity via the reputation (and trust) of the signing CA. In addition to the user's identity and public key, digital certificates also hold other relevant information; e.g., a user's company affiliation information, expiration date, usage, the issuer of the certificate, and the degree to which an identity check was conducted on the users, and so forth. The exact contents of any certificate are flexible, and determined by the policy of the organization that enlists a CA to provide the necessary fields and values to support their infrastructure. This information is found in the organization's Certificate Policy (CP). Figure 7 illustrates a certificate:

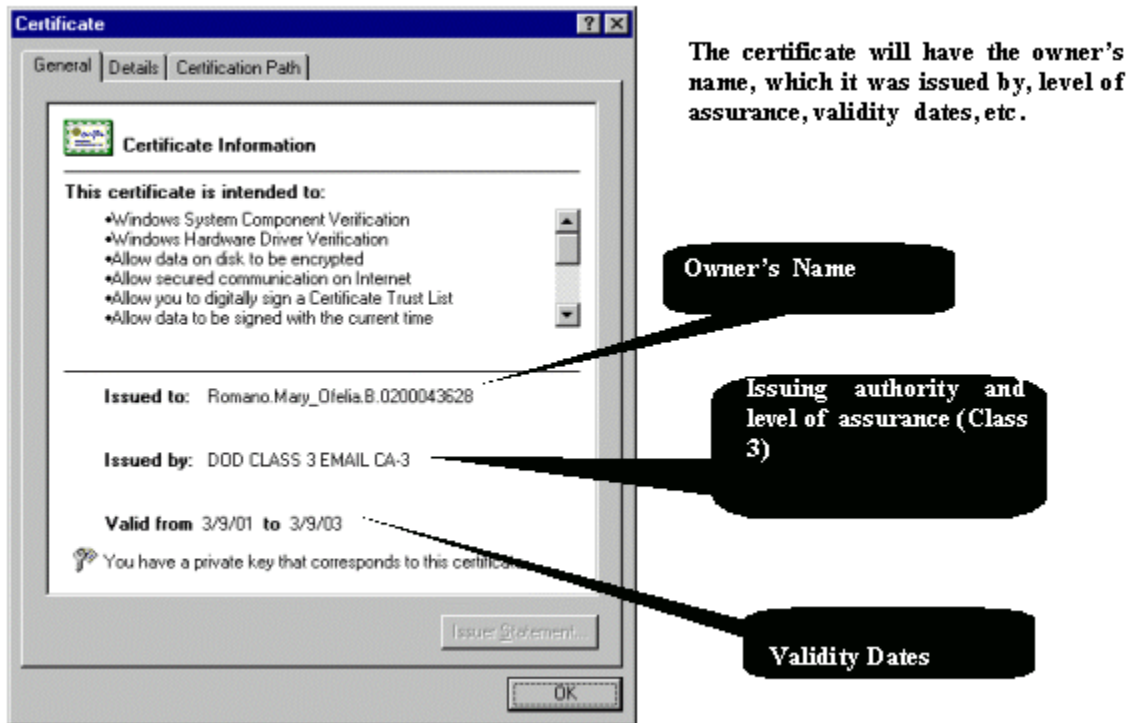


Figure 7. Digital Certificate [From: 1, Slide 21]

A digital certificate can be used by other users to verify that a public key belongs to a specific individual, as long as the issuer of the certificate is trusted. Therefore, if a user wants to send an encrypted message to another person, the recipient's name is looked up in the directory of a Certificate Authority and then downloaded to her workstation so she can use the enclosed public key to encrypt the message.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OVERVIEW OF PKI

Living in the Internet era has increased the importance of, and requirements for, information security; especially within large information-intensive organizations such as the DoD. In order to meet these requirements, the DoD decided to develop and implement a Public Key Infrastructure (PKI) as a way of securing information that is exchanged either through its own networks or through the public Internet.

A. WHAT IS A PUBLIC KEY INFRASTRUCTURE (PKI)?

The term PKI can be very confusing because it is used to mean several different things. On the one hand PKI may mean the methods, technologies and techniques that utilize public key encryption to provide a secure infrastructure (a “macro-level” interpretation). On the other hand, it may mean the use of a public and private key pair for authentication and proof of content (a “micro-level” interpretation).

PKI is a security architecture that was introduced to provide an increased level of confidence for exchanging information over an insecure internet. In this section, the reader will be presented with a basic overview of the public key (PK) infrastructure and the key terms and concepts used in a PKI. Many different answers exist for the question “What is a Public Key Infrastructure?” A few of them are discussed below.

Public Key Infrastructure refers to

...the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates, and provides that critically needed support to applications providing confidentiality and authentication of network transactions as well as data integrity and non-repudiation. The PKI encompasses Certificate Management and Registration functions. (Public Key Infrastructure Roadmap for the Department of Defense May 7, 1999) [1, (Slide. 2)]

A PKI is “...that portion of the security management infrastructure dedicated to the management of keys and certificates used by public key-based security services.” [8, p. 2-5]

A PKI is "...personnel, policy, procedures, components and facilities to enable public key cryptographic functions so that applications can provide the desired security services." [5, p. 15]

Essentially, a PKI includes all the components required to establish and maintain the trust relationship and the binding of a public key to its owner within a system providing public key-based applications. "Most important is the fact that with IT security, just as with military security or castle fortification, security is only as good as its weakest components." [9, pp. 23-24]

B. WHAT CAN YOU DO WITH A PKI?

A Public Key Infrastructure lets an organization such as DoD take advantage of the speed and immediacy of the Internet while protecting critical information from interception, tampering, and unauthorized access. A PKI provides the following capabilities:

- Communicate securely with an organization's employees around the world. A PKI offers remote users with secure channels to their home intranets.
- Exchange confidential data with an organization's business partners. A PKI supports the creation of secure extranets that give select partners easy access to business-critical information stored on an organization's internal network.
- Take advantage of secure e-commerce. PKI lets you offer a world of customers the confidence to purchase your goods and services on the Web.

In more analytical terms, a PKI infrastructure is expected to offer its users the following benefits:

- *Authentication* - proof that the sender is whom he claims to be
 - Digital certificates issued as part of an organization's PKI allow individual users, organizations, and website operators to confidently validate the identity of each party in an Internet transaction.
- *Privacy (Confidentiality)* - assurance that only the intended recipient is able to decrypt the sent message
 - Public key encryption protects information from inspection during transmission.

- *Authorization* - protect against unauthorized use
 - PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet log-in security (access authorization).
 - With PKI solutions, an organization can control access privileges for specified online transactions (transaction authorization).
- *Integrity* - verification that no un-detectable modification of data has taken place during storage or transmission across the network.
 - A digital certificate ensures that the message or document the certificate owner "signs" has not been changed or corrupted.
- *Non-Repudiation* - assurance for the legal community that the person sending cannot deny participation.
 - Digital certificates validate their users' identities, making it nearly impossible to repudiate a digitally "signed" transaction later.

Table 2 illustrates the basic security services provided by a PKI.

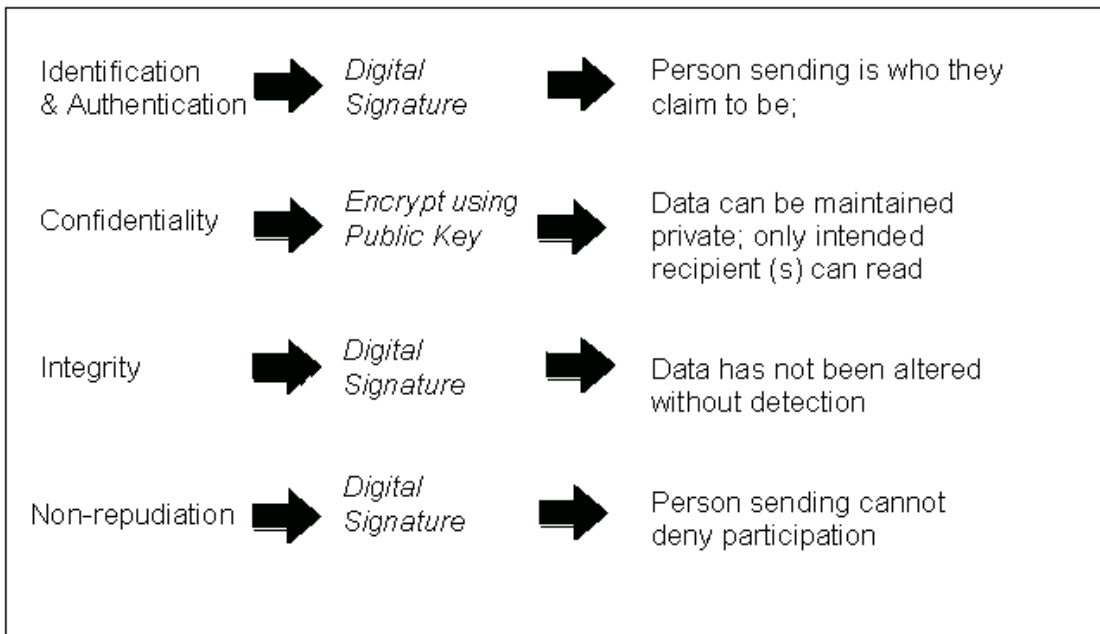


Table 2. PKI Security Services [From: 10, Slide 8]

C. CERTIFICATES

In the section on public and private keys, references were made to certificates. Here the place of certificates in the public key infrastructure will be further expounded. There are some problems regarding public key usage, such as how users can “carry” and manage many, and how they can be sure that each key truly belongs to its claimed owner. Certificates and Certification Authorities are used to answer these questions and build confidence into a public key infrastructure.

Figure 8 illustrates the various fields referred to in a certificate:

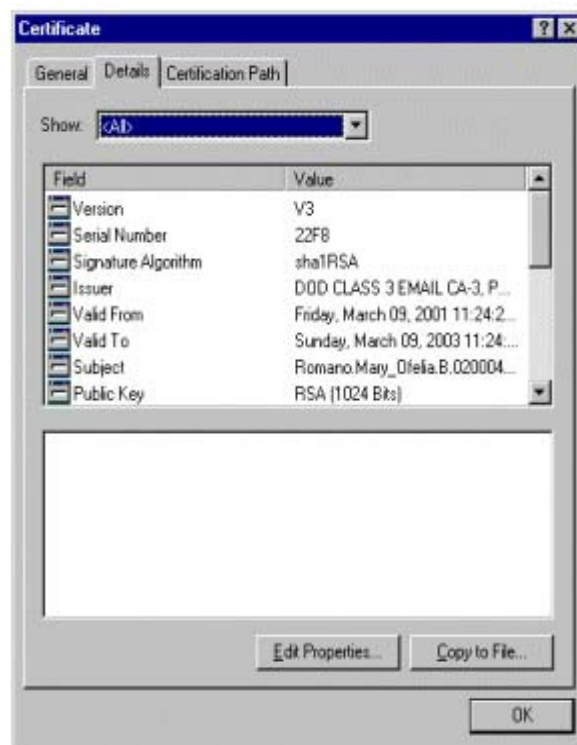


Figure 8. Figure Certificate Fields [From: 1, Slide 22]

In the DoD environment four (4) types of certificates are issued:

1. Identity

This certificate is used to digitally sign documents or electronic forms and to authenticate (prove a claimed identity) the user to applications. Each individual will have, at a minimum, an Identity certificate.

2. E-Mail Signature

This certificate is used to digitally sign e-mail messages. This is only required if the user’s organization is using a PKI-enabled E-mail application.

3. E-Mail Encryption

This certificate is used to digitally encrypt e-mail messages. This is only required if the user’s organization is using a PKI-enabled E-mail application.

4. Server

Certain DOD servers, such as private web servers, will be required to have their own identity certificates to properly identify the server on the network and to provide secure, encrypted communications.

Table 3 summarizes the use of certificates:

Type	Facilitates
Identity	Authentication, Non-repudiation, and non-e-mail digital signature
E-mail Signature	Authentication, Non-repudiation, and e-mail digital signature
E-mail Encryption	Encryption of electronic transmissions for greater security and confidentiality
Server	Enables SSL Encryption of Web Server Content

Table 3. Certificates Usage [From: 11, Slide 8]

D. MAJOR COMPONENTS

A PKI is created by combining a number of services and technologies. The major components are introduced and discussed in the subsections that follow. The basic relationship between all of the services is illustrated in Figure 9.

A CA may also state the quality of the checks conducted before the certificate was issued. Different classes of certificates can be purchased that correspond to the level of checks made. There are four general classes of certificates.

- Class 1 certificates can be easily acquired by supplying an email address.
- Class 2 certificates require additional personal information to be supplied.
- Class 3 certificates can only be obtained after more thorough checks have been made of the requestor's identity.
- Class 4 certificates may be used by governments and organizations needing very high levels of identification verification.

The revocation information provided by the CA's about revoked certificates lets users know when certificates are no longer valid. This can be done in one of two ways: 1) Certificates can be deleted from the directory or database in which they should be found. As a result, any attempt to find them to check that they still exist will fail and anyone looking for them would know that they have been revoked. 2) A system of revocation lists (CRLs) has been developed that exists outside the directory. This is a list of certificates that are no longer valid (no matter the reason).

2. Registration Authority (RA)

A CA typically employs one or more separate facilities, called Registration Authorities (RA) to perform the necessary identity checks on certificate applicants. A RA authorizes the creation of a certificate and provides identity validation information to the CA. Depending upon the specific infrastructure; it may also be the RA (or LRA) that also sends the applicant's public key to the CA to have it certified and place in a certificate. RA's are also responsible for administering any Local Registration Authorities that are deemed necessary, and serve as reporting point for the notification of revocation requests.

3. Local Registration Authority (LRA)

Like RA's, LRA's are responsible for registering applicants. They authorize the creation of a certificate and provide the requisite information to the CA.

Users are required to prove their identity using their ID cards. Once the identity is verified, the LRA then registers the user and shows them how to generate their key pair and obtain their certificate from the CA. LRAs are established only in larger PKI's where users are expected to be spread over a wide geographic area, and would therefore benefit from the accessibility of a local office that handles the registration and user-level administration of the infrastructure on behalf of the superior RA.

4. Directory (or Repository)

Directories are one of the vital elements of any PKI. The CAs publish certificates and CRLs to these directories. In this manner, a user can retrieve the certificate of any other user who was issued a certificate by the directory owning CA. These directories store all current certificates and current certificate revocation lists.

Directories are databases that contain certificates. In the DoD implementation these certificates are predominantly in the X.509 format. They may be made publicly available or may be access-limited to a specific organization. For example, a company may have its own directory where it holds certificates for the exclusive use of only its users.

5. Users

Users are all people (DoD personnel), devices or applications, that will be issued certificates (certificate owners), or will utilize the certificates of others (relying parties). All users who are issued certificates are expected to keep the associated private key confidential.

Figure 10 illustrates the relationship among PKI components.

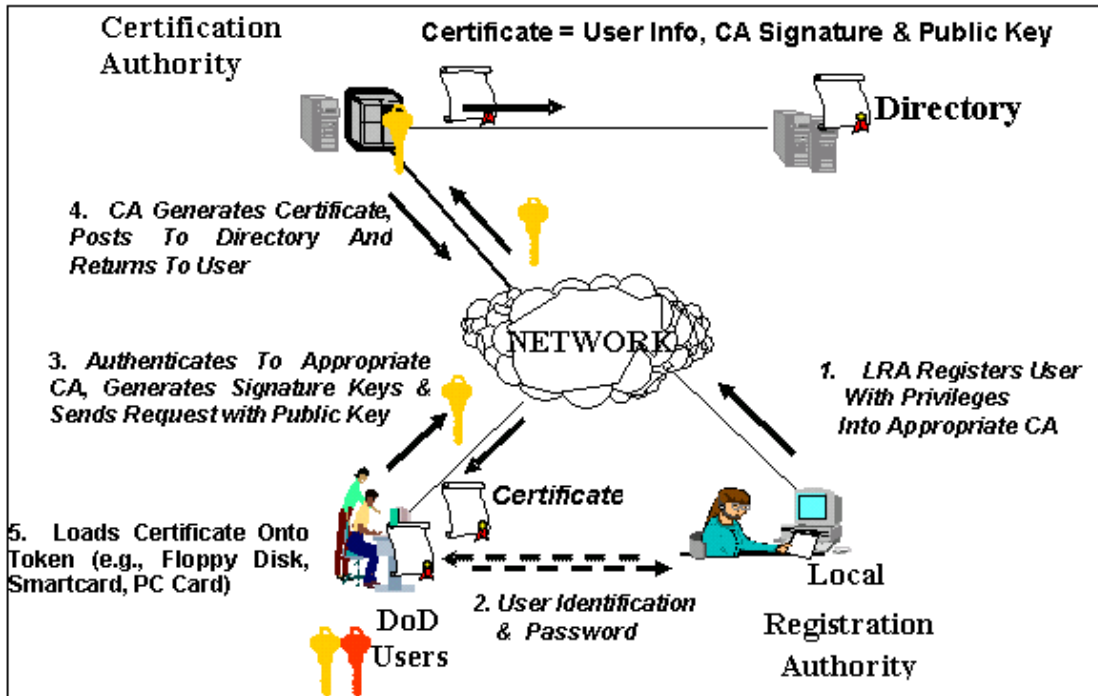


Figure 10. User Registration [From: 1, Slide 33]

E. CERTIFICATE REVOCATION LISTS

Previous paragraphs mentioned that a certificate contains an expiration date. In addition, a certificate may become invalid before the expiration date occurs. Since the entire infrastructure relies upon certificates' validity, a system has to exist which allows participants to know when certificates have been invalidated prior to their normal expiration date. Consequently, CA's need a mechanism to provide a status update for the certificates they have issued and published.

One approach to solving this issue could be to delete certificates from the directory or database in which they should be found. As a result, any attempt to find them to check that they still exist will fail and anyone looking for them would know that they have been revoked. There are three problems with this approach.

- A denial of service attack on the directory or database might create the false appearance of a failed certificate.
- Deleting the record does not tell the person asking for the information why it is not there, which may be important depending upon local policy regarding the reason for revocation.

- Many implementations of the PK Infrastructure will result in certificates being cached (i.e., copied) in multiple locations; thus complicating the simple solution of simply deleting certificates only from the CA's directory.

As a result, a system of managing revocation lists has been developed that exists outside of the certificate directory/database.

A Certificate Revocation List (CRL) is a computer generated list of certificates that have been revoked by the issuer prior to their original expiration dates for some reason. Revocation lists are periodically issued by each certificate authority and published to the directory. Accessibility to the revocation lists is of paramount importance to the trust required of the infrastructure, as relying parties must ensure that the certificates they use have not been revoked. Thus, these lists should be available at all times, even when their corresponding certificate directory may not be available. In other words, the inability to obtain a certificate is deemed less problematic than the inability to verify the status of a certificate.

Certificates may be revoked for a variety of reasons, including:

- Key Compromise – there is reason to believe the token on which a user or other end-entity private key resides or a copy of the private key, in the case of software tokens, has been obtained by an unauthorized individual.
- CA Compromise – there is reason to believe the token on which the CA private key resides has been obtained by an unauthorized individual.
- Affiliation Changed – the user has terminated the association with an organization listed in the Distinguished Name field in the certificate. Position changes within an organization do not require revocation of a certificate.
- Superseded – a replacement certificate has been issued to a user, other end-entity, or CA and none of the above reasons are applicable. Examples include that the token has failed, the user has forgotten the password to unlock the token, there is a change in legal name or a change in unique identifier.
- Cessation Of Operation – applies to CA certificates. The operation of the CA has been terminated. Note that if a CA no longer issues certificates, but remains capable of issuing CRL's, its certificate need not be revoked and certificates issued by the CA may continue to be used.

Thus far we have examined the PKI, its components and how all of these work together. In the next chapter we will discuss the DoD effort to optimize PKI security via use of smart card technology, specifically, the adoption of the standardized Common Access Card (CAC).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE COMMON ACCESS CARD

Even though DoD gained numerous benefits from the incorporation of public key cryptography techniques, some problems have arisen that are associated with the specific requirements that DoD has defined. These problems arise from the added complexity involved in managing the plethora of keys. Smart cards were conceived as an alternative that could help securely manage both private and public key (i.e. certificate) management, providing both convenience and security while minimizing the users' need to expose personal and private information. Since the smart card is an active device (i.e., it is capable of processing data via an onboard processor), it is able to restrict the information it provides to only that is required for the specific service(s) for which it is intended to interface with. In addition to information security, smart cards achieve greater physical security of services and equipment, because the credentials on the card provide a relatively strong authentication mechanism (i.e., what you know—a PIN—and what you have—the card) for access to physical facilities.

A. INTRODUCTION

A smart card is a type of plastic card embedded with a computer chip that stores and processes data on behalf of the card's owner and computer system he is interacting with. Pertinent external data (e.g., the hash of a document to be signed) is transferred to the card and processed within the card's microprocessor chip. User or application-specific data or programs stored on the card are accessed via a peripheral card reader device that acts as a conduit between the functionalities provided by the card and various network applications. The cards greatly improve the convenience and security of cryptographic transactions and they provide somewhat tamper-resistant storage of the owner's cryptographic credentials. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Smart cards can also serve as a means for network system access, and can store other personal data such as; medical, security clearances, authorizations, biometric information, payroll information, etc.

Smart card-enhanced systems are in use today, and to varying degrees, all applications can benefit from the added features and security that smart cards provide. People worldwide are now using smart cards for a wide variety of daily tasks. Most of these tasks revolve around some implementation of securing information and/or physical assets.

B. BACKGROUND

Since 1993, the DoD has been conducting evaluations on smart card technology. Initially tested as an updateable, individually carried, data storage device, the Department's smart card mission has evolved to require an interoperable, backward compatible device for secure on-line data transfer and on-line transactions. After detailed testing and many pilot demonstrations, this effort resulted in a decision to implement smart card technology as a Department-wide Common Access Card (CAC).

The CAC will be the standard ID card for active duty members of the Uniformed Services, Selected Reserves, DoD civilian employees, and eligible contractor personnel. The CAC platform will contain the identification credentials, encryption keys, encryption ciphers, digital signing certificates, and may also contain Department-wide and/or Component-specific applications; e.g., deployment readiness, or dental and medical information. The CAC will also be the principal card used to enable physical access to buildings and sensitive spaces; as well as for logical access to the Department's computer networks and systems. In addition, more applications³ are being developed and targeted for post-issuance download to the CAC.

The CAC is being implemented by the Defense Manpower Data Center (DMDC) and maintained using the infrastructure provided by the Defense Enrollment Eligibility Reporting System (DEERS), which acts as a data warehouse for all the military and civilian personnel databases in the Department. DEERS is bound to the DoD PKI Certificate Authorities (CA's) to provide the trust that a person holding a CAC is affiliated with the DoD. The system is "aware" of every card issued and currently active. Strong security safeguards are present during the issuance process to prevent the

³ These are Java, Service-specific applets that would be downloaded via a web browser.

counterfeiting or theft of cards. As can be seen, the DoD CAC deployment establishes an issuance environment which provides the DoD a strong level of assurance that only properly identified and authorized individuals are carrying a Common Access Card.

C. CONTENT

Smart cards incorporate 2-factor authentication: something that you have (the card) and something you know (the PIN). In addition, smart cards have secure, tamper-resistant memory to store sensitive information, such as private keys, and can perform cryptographic computations entirely within the tamper-resistant microprocessor.

Smart cards have the capacity for greater storage space than the more traditional magnetic stripe cards, are more reliable, perform multiple functions, and are more secure because of the use of security mechanisms such as advanced encryption and biometrics. Due to the card's self-contained processing capabilities, it can process transactions with a connected computer onboard. That is, on the card's chip rather than relying on the attached computer.

A smart card is a credit card-size device, carried and used by DoD personnel, which contains an integrated circuit and may also employ one or more of the following technologies:

- Magnetic stripe,
- Bar codes,
- Biometric information,
- Encryption and authentication, and
- Photo identification.

Figures 11 and 12 show the outer view of a CAC:

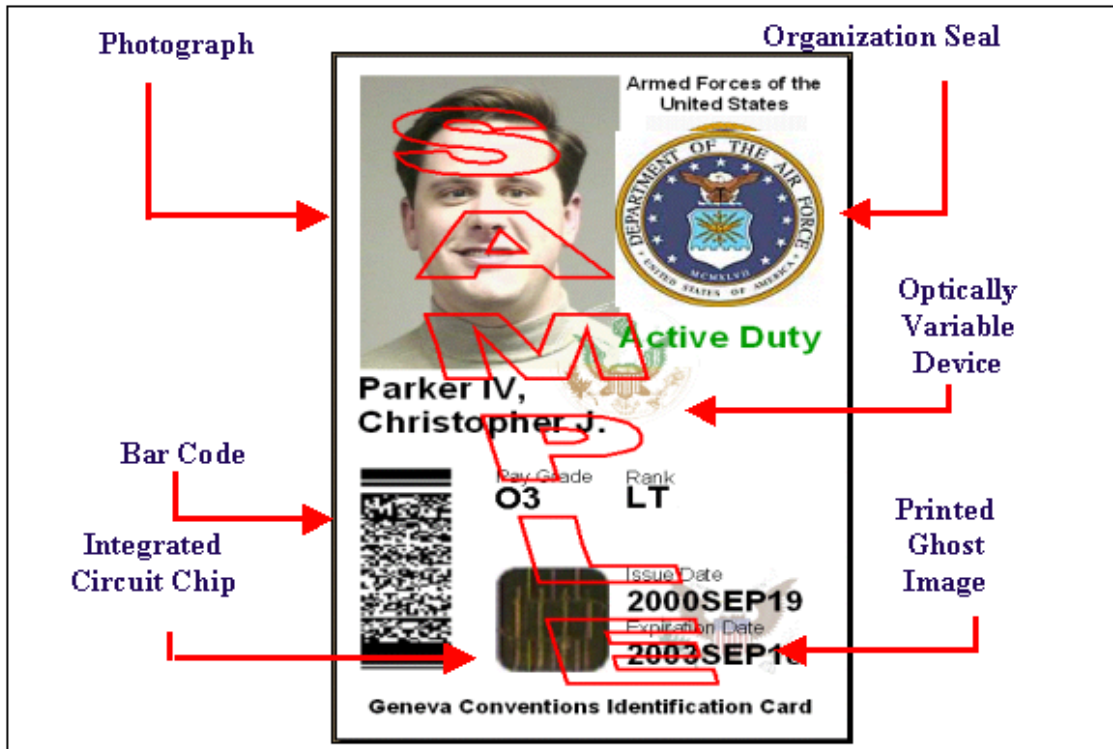


Figure 11. CAC Front View [From: 11, Slide 11]

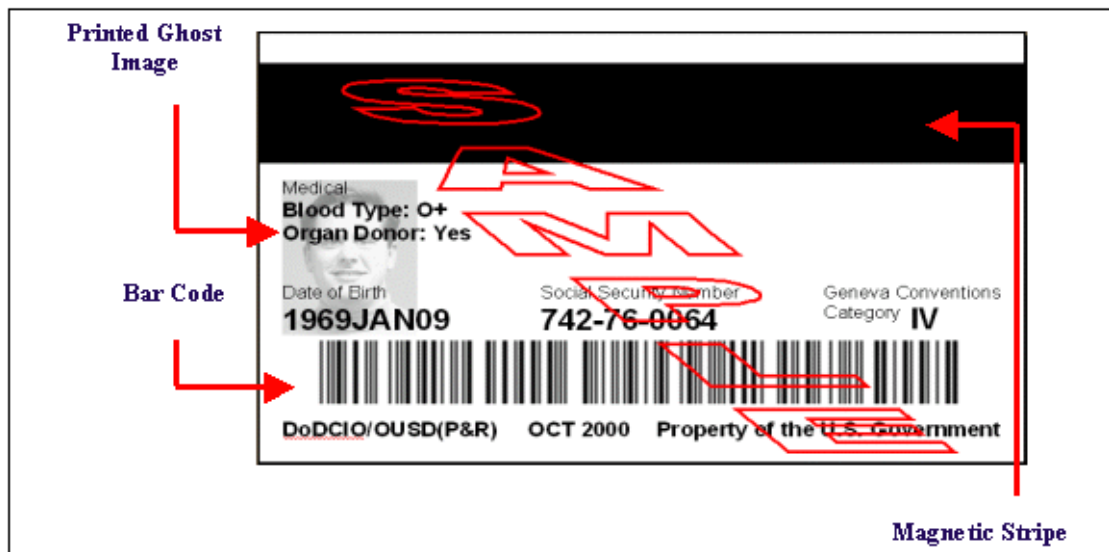


Figure 12. CAC Rear View [From: 11, Slide 12]

D. DOD AND THE COMMON ACCESS CARD (CAC)

As already mentioned in previous paragraphs, the Department of Defense (DoD) has chosen the Common Access Card (CAC) as its solution for the adoption of smart card technology.

The Common Access Card (CAC) will perform the role of a new ID card (identification card), for DoD personnel. Due to its advanced capabilities, the card can:

- Authenticate for physical access to restricted buildings and other sensitive spaces,
- Control access to computer networks and systems, and
- Serve as the primary platform for its owner's keys and certificates, facilitating simplified log on and digital signing.

Figure 13 summarizes the main components of CAC:

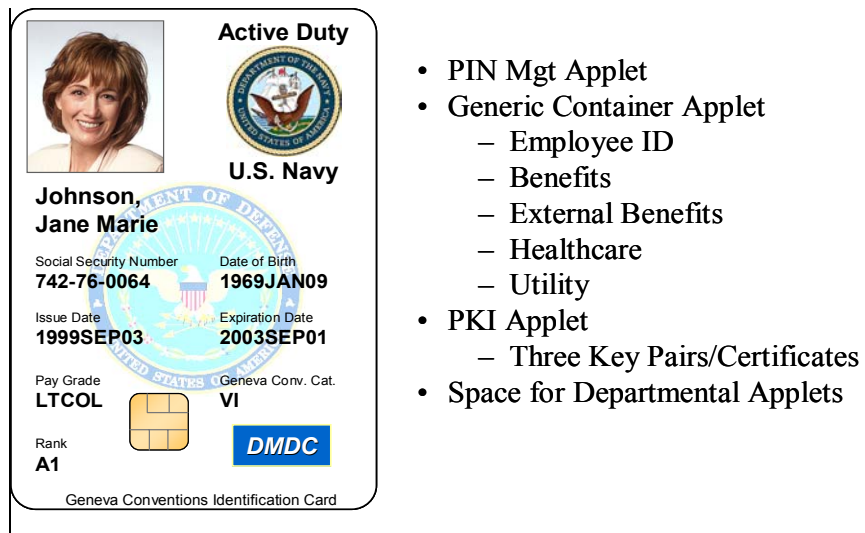


Figure 13. CAC View. [From: 13, Slide 2]

1. Benefits of the CAC

Many advantages will be gained with the CAC implementation within the DoD environment. These include:

- Increased protection for personal and national security through the Public Key Infrastructure (PKI)⁴. PKI adds an extra layer of security, because without the CAC, no one can log onto a user's computer even when possessing the name and password.
- Bureaucracy reduction since many paper-based processes may now become automated.
- Help some commands with day-to-day business to reduce their employees' "hurry up and wait" time, or otherwise improve their work efficiency.

2. Common Access Card's Design

The CAC is a Java-based integrated chip (IC) microprocessor card. It contains three (3) kinds of memory:

- **ROM (read-only memory)**, which contains the CAC operating system, written to the chip during the fabrication process,
- **RAM (random access memory)**, which is used as a temporary working space for storing and modifying data, and
- **EEPROM (electrical erasable programmable read-only memory)**, which is used for data storage and user applications and can be written to after the card is made.

The CAC's EEPROM is divided into two security domains.

- The first security domain is reserved for the Department's PKI, demographic, and middleware data and applications. These are instantiated on the card during the initial CAC issuance to DoD personnel.
- The second security domain is used for service-specific Java applications known as applets. These are written to the card post-issuance. The service-specific space is a reserved area available to DoD divisions and departments for unique applets that are custom built and serve a specific purpose. In addition, Java applications are being developed and targeted for post-issuance download to the Common Access Card.

Figure 14 illustrates the location of CAC domains within the card:

⁴ PKI is a CAC component, and is an enabling technology that provides data protection through authentication and data integrity. PKI performs specific functions such as single sign-on access control, signing electronic documents, and encrypting email.

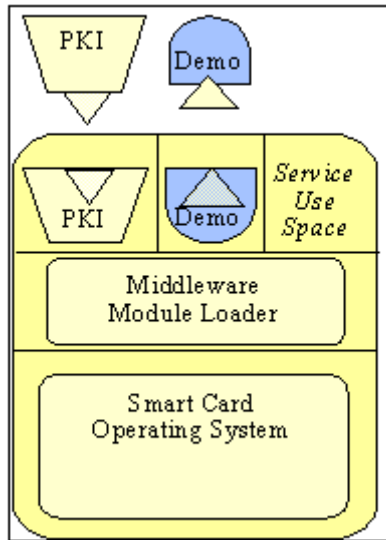


Figure 14. Chip Allocation [From: 14, p. 1]

3. CAC Functionality

The Department of Defense Common Access Card (CAC) was developed to meet three requirements of the Department:

- A digital signing credential that meets the legal requirement of non-repudiation to enable e-business initiatives,
- A hardware token for DoD PKI to meet the department's security requirements for unclassified networks protection, and
- Smart card technology that was proven to enable the re-engineering of business processes resulting in improved readiness and quality of life, efficient and paperless business processes, and cost savings.

A smart card with a crypto co-processor and on-card key generation could meet all three of these requirements. The decision to implement smart card technology included certain mandated requirements for this card.

Smart cards incorporate a 2-factor authentication: something that you have (the card) and something you know (the PIN). In addition, smart cards have secure, tamper-resistant memory to store sensitive information, such as private keys, and can perform cryptographic computations entirely within the tamper-resistant microprocessor.

The information on the card is securely stored and is not viewable by the card holder. Since the private key is stored in tamper-resistant memory of the card (it never

has to leave the card), the smart card needs to be protected with physical and cryptographic protection measures. Furthermore, it will never be seen by the card holder. All the cryptographic functions that require the use of the private key, such as digital signature creation, will take place on the card.

The public key is sent (emitted) to a Certification Authority in order for a digital certificate to be created.

Only individuals and applications that have authorization can access and read the information on the CAC. CAC holders can release their information using their personal identification number (PIN) at facilities configured to utilize CAC-based applications.

Since a smart card is portable, the private keys and digital certificates can be with the cardholder at all times and at all locations.

As for PKI support, the CAC carries Identity, Digital signing and E-mail keys/certificates used for encryption, digital signing, and authentication. A brief discussion of the three certificates stored on the CAC appears below.

- Identity certificate: the identity credentials are used for secure authentication. The key pairs may be generated on the card. This is a policy decision that needs to be made regarding whether to mandate the use of on-card key generation
- Digital signing certificate: the digital signing credentials are used for digital signature functions.
- E-mail (encryption) certificate: the e-mail encryption credentials are used for e-mail encryption functions. These key pairs are generated in the client workstation's software cryptographic module, although they can be generated on the card.

Figure 15 illustrates these key pairs/certificates:

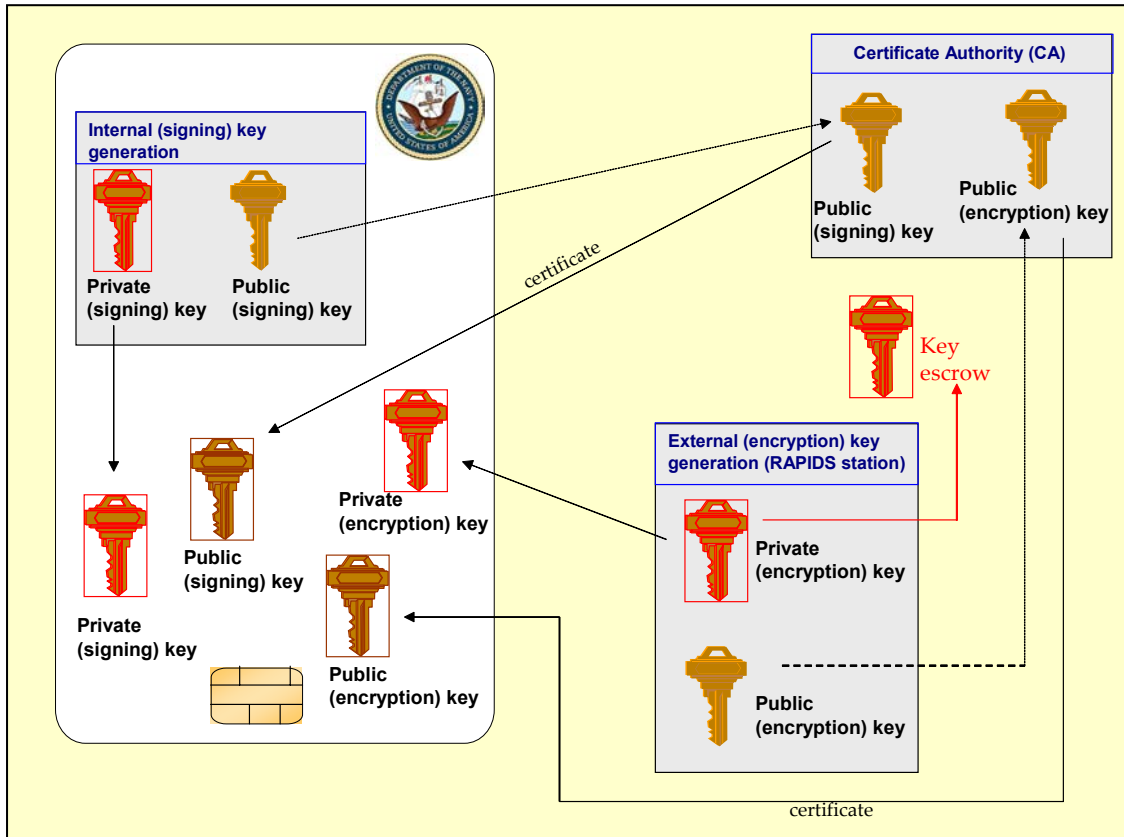


Figure 15. CAC Card's Key Pairs

From Figure 16 it can be ascertained that:

- Both public keys are available for certificate generation
- The key pair used for digital signatures is generated inside the card. The private key is directly written to the card and cannot be read. The matching public key is transmitted out of the smart card, allowing a request to a CA for a digital certificate to be made.
 - The corresponding private (signing) key is used to create the user's digital signature.
 - The public (signing) key is used from the recipients to verify the user's digital signature.
- The key pair used for data or e-mail encryption is generated outside of the card in the RAPIDS station. After the key's creation, the public (encryption) key is sent to the CA allowing a request for a digital certificate to be made. The CA digitally signs the certificate and sends this certificate and the associated keys to the card for storage.

- The public (encryption) key is used to encrypt a user's data.
- The corresponding private (encryption) key is used to decrypt encrypted data. A copy of this key is *escrowed* by the CA⁵

Figure 16 illustrates the usage of a CAC or how a card holder can send a secure message to a recipient.

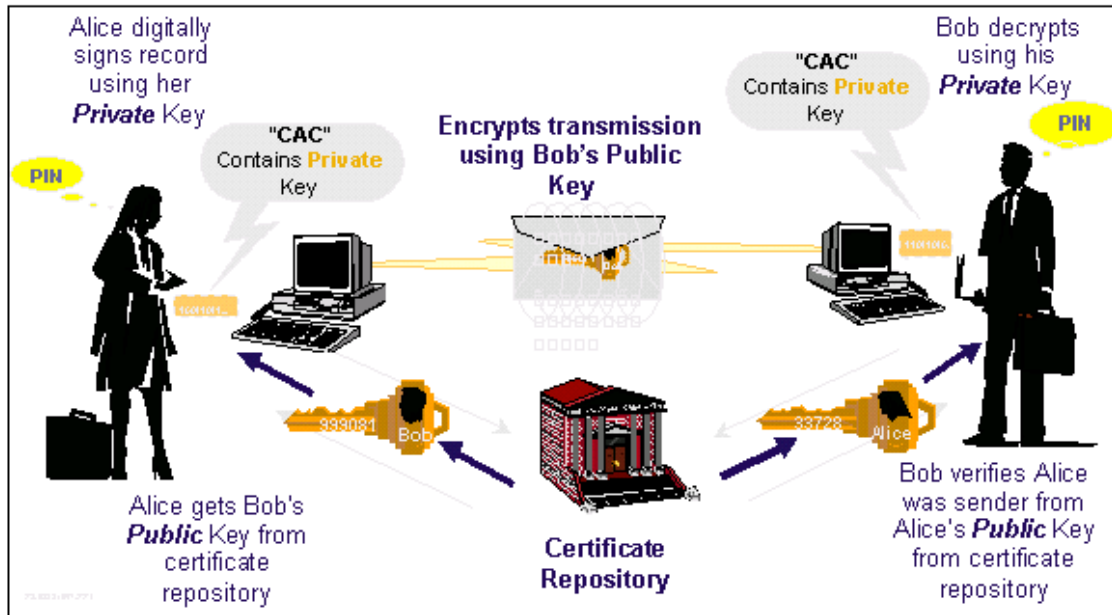


Figure 16. Digital Signature and Encryption [From: 11, Slide 15]

Thus far we have examined the operation of the overall infrastructure (Chapter III), and the design, function and benefits of integrating the CAC into this infrastructure (Chapter IV). From the CAC issues described above, it can be seen that building such a complex system, especially within the complex DoD environment, is a difficult task which requires thorough user understanding. The next chapter will argue for the need and the importance of user understanding.

⁵ That is, it is saved at another secure location and can be used from an authorized entity (such a CA) for recovery purposes.

V. TRAINING FOR THE DOD PKI

This chapter will provide some reasonable justification for the importance of personnel training within the DoD environment. The manner in which personnel will use the DoD PKI will affect the integrity of the whole infrastructure⁶. Thus, the human factor will play a vital role in the integrity and success of the overall infrastructure.

A. THE TRAINING NEED

As is already known, the success of implementing a PKI is based completely on the trust between the components of the infrastructure. As seen in the previous chapters, if this trust cannot be established, PKI cannot provide the designed and intended services and levels of assurance, and therefore, the system's integrity will be threatened. It is imperative that the system's integrity be supported and maintained by the correct usage and implementation of technologies and policies. These technologies and policies will provide the necessary framework on which the system's integrity will be based. Training will be helpful in overcoming the human-centric obstacles that arise from implementing a relatively new and complex system⁷.

One of the most important factors of a successful PKI implementation is user training. For an organization the size of DoD, this is a challenging problem,⁸ and not only because of the large number of users, but also because most of those users do not have a strong background in the underlying cryptographic technologies.

⁶ "Most important is the fact that with IT security, just as with military security or castle fortification, security is only as good as its weakest components." [Austin, T., PKI: A Wiley Tech Brief, John Wiley & Sons, Inc., New York, NY, 2001, (p. 23-24)]

⁷ "Underlying a successful policy are resources to support enforcement, educate users, and modify the environment as external and internal conditions change." [Austin, T., PKI: A Wiley Tech Brief, John Wiley & Sons, Inc., New York, NY, 2001, (p. 26)]

⁸ It is estimated that over three million certificates will be required for the DoD PKI implementation [Green, R. M., "Public Key Infrastructure: The Enabler for DoD e-Bus," January 2001]

B. CURRENT TRAINING STATUS

Within the DoD environment, much effort has been expended to develop various tools that will provide training and a better knowledge of PKI concepts to the average user. However, these efforts have been pursued somewhat parochially by the different services, and based upon the different needs of these services.

This has led to the existence of a large number of training resources, which in turn caused, or still causes, misunderstandings among the PKI users. In the DoD environment, there are many resources which can be used for training DoD personnel. These resources can be found in a wide variety, such as text documents, slide presentations, interactive CD-ROMs, video tapes and many websites. Many of these can be downloaded, or viewed online. This variety can be problematic, especially for un-trained users that do not yet have sufficient knowledge to distinguish core concepts of public key cryptography from service-/agency-specific details.

Here are two typical sources through which DoD users can find various information and training materials:

- The DISA (Defense Information Systems Agency) website (<http://iase.disa.mil>). Through this website, it is possible to have access to various PKI information, including training materials, and information on RA/LRA training courses offered.
- The SPAWAR (Space and Naval Warfare Systems Command) website, which provides much information such as, public key cryptography overview and basic concepts of PKI, and training courses for RAs and LRAs.

Finally, there is a new philosophy in the DoD environment, and primarily in the U.S. Navy, suggesting that instead of centralized PKI training, the PKI training is instead an added feature to every PKI-enabled application.

C. A DOD PKI AND CAC INSTRUCTION TOOL

1. Why Web-Based Training

Nowadays, the use of the Web is still gaining a lot of attention and is growing day by day. Therefore, in the opinion of the author it is clear that any training effort would be more dynamic and available if it is packaged for delivery on the Web⁹ instead of the more traditional hardcopy print format.

The benefits of Web-based training include accessibility and similarity of provided training, since every user; either from home, office, or any other place in the world; can complete the training as long as he/she has an Internet connection and a computer with a Web browser and the same material is available to all users and presented in the same manner.

While traditional classroom instruction has the student listening without participating; Web-based delivery has the student more actively participating in the learning process. The user has more freedom in choosing the time of study, length of study, pace of study per session, and content of study.

Due to frequent changes in technologies, an easy way of updating the presented material is provided. Therefore, all users will be current on the most recent changes since new content can be updated on the server and thus be immediately available to them. Due to the large number of DoD users and their wide dispersion throughout the world, this feature becomes even more attractive.

This approach provides numerous controlling and monitoring capabilities that can be useful for checking user progress through the training process, e.g., which user is accessing the material, when it was accessed, or the level of performance. Therefore, valuable information regarding user statistics can be collected and used for further improvements.

⁹ Web-based training is instruction that is delivered via a Web browser such as Microsoft Internet Explorer or Netscape Navigator through the Internet or corporate intranet. It offers online classes with facilities for interacting with a live instructor and other students or simply as independent study in which the students work on their own with, perhaps, contact through e-mail and real-time 'chat' with the tutor and other students. [Steed, C., Web-based Training, Gower Publishing Limited, Brookfield, VT, 1999, (p. 28)]

Finally, due to reduced redundancies of material, and the self-teaching nature of a Web-based tutorial, cost reductions can be achieved. Specifically, there is no need for buildings, classrooms, transportation, lodging accommodations, etc. Users will spend less time training compared to the conventional method of attending in a classroom. Also, there is no need for extra expenses for special hardware and special training software. All users can take advantage of the already existing technology and hardware; with just a computer, an Internet connection or an intranet access and with a Web browser users can have access to the training material. Additionally they can take advantage of pre-existing software and tools, which can be useful for developing the Web-based training material.

However, because nothing is ideal, Web-based training also has some disadvantages [15]. These disadvantages stem from various factors that can affect the efficiency of this type of training.

It must be emphasized that it is not a simple task to design and develop a Web-based course and sometimes it can be a very intensive and painful procedure which might require the efforts and the cooperation of several people if high quality material is expected. Furthermore, although nowadays the use of computer and Web technology has grown, in some organizations a redesign of their training procedures might be required in order to achieve their intended goals and to establish a new mentality among their members.

In order to be more efficient, the Web-based training should be accompanied by some lab training material, so the users will have the opportunity to check their knowledge status after the completion of their training. The absence of personal contact with an instructor is another disadvantage, especially for users who are more accustomed to this traditional way of teaching (for this reason, some systems allow communication with an instructor, through e-mail, for example).

Finally, due to the fact that many users do not have “fast” network connections, resulting in bandwidth problems concerning the volume and processing requirements of the training material.

In the author's opinion, the disadvantages of Web-based training are less and insignificant relative to the obvious advantages of this training method, especially when discussing DoD.

Finally, before making the decision on whether to adopt Web-based training, some other factors¹⁰ must be taken into consideration. These factors include the organization's geographic location and the size of trainee audience, since distributed learning can be a much more efficient approach for organizations with geographical dispersion and with many people to train.

Also, the type of provided material is a critical factor, since material with a dynamic nature, such as fast-changing methods, procedures or products, it is important to be up-to-date with the latest changes. This way, trainees will be kept with the most recent material.

In the author's opinion, developing a Web-based training tool is a worthwhile effort based on all the aforementioned reasons, which will benefit the DoD PKI and all its users.

2. PKI and CAC Instruction Tool General Overview

In this section, a presentation and description of the provided Web-based training tool will be given to include its features and details. Its basic features and characteristics are:

- It can be easily accessed through an Internet connection and the use of a Web browser using either Microsoft Internet Explorer or Netscape Navigator¹¹.
- It is centrally located and managed. The benefit of a centrally maintained site has already been described in previous paragraphs.
- It provides information about PKI-enabled applications.
- It provides supplementary and amplifying information via hyperlinks to pertinent reference material.
- It can be used by users as a reference and help tool by providing access to specific information.

¹⁰ These factors are thoroughly presented in Steed's book Web-based Training [Steed, C., Web-based Training, Gower Publishing Limited, Brookfield, Vermont, 1999].

¹¹ It can be used for downloading keys and certificates within the DoD PKI.

This instruction tool provides a basic overview of the PKI and CAC concepts and does not provide specific implementation, or policy-specific details. Obviously, there is a lot of room for both future improvements and upgrades especially as technology goes further, and the accomplishment of more detailed training on specific topics. However, this is beyond the scope of this thesis.

D. INSTRUCTION TOOL DESIGN AND DEVELOPMENT

The main concern during the development of this training tool was the simplicity and the ease of use for the end user. Therefore, during the design, a continuous effort was made to keep the tutorial uncomplicated and user-friendly. Features contributing to this goal include an easy-to-use interface, well-organized material, use of multimedia, and ease of link and page navigation.

1. Goals and Required Functionality

The goal of this instruction tool is to provide information about the DoD PKI and the CAC (Common Access Card) concepts, by giving to users an instruction tool capable of providing all DoD CAC holders with the rudimentary knowledge of how their CAC fits into the broader DoD PKI infrastructure. This web-based tutorial requires no instructor, and presents a validation test to each user (via a web browser and an Internet connection). Because DoD personnel comprise a large and varied group of people, with different knowledge levels and skills, the tutorial's interface to the provided tool must be kept simple, comprehensible, user-friendly and easy to use from users with a minimum level of computer skills.

This instruction tool will provide training on particular topics, provide the functionality to test users' knowledge, and support the tracking of completion and evaluation (i.e., test) results.¹²

¹² The tracking capability is essential for effective management of users (i.e. before being issued a CAC card an end user would be required to complete basic training and successfully complete a test on the material.

2. Tutorial's Design

The effort of developing the DoD PKI and CAC instruction tool which took place in this thesis, attempted to incorporate some common sense design characteristics for web-based instruction delivery. The attempt was to generate a user-friendly and helpful tutorial's web interface. This can be achieved by explicitly defining the scope, the objectives, and the provided training material of final delivery.

In accordance with the goals described in the previous paragraph, the substance of the DoD PKI and CAC instruction tool is the information which is presented in the form of short (approximately one "web" page) lectures. The tutorial allows users to follow a series of lectures which present definitions and explanations about cryptography (symmetric and asymmetric), digital certificates, PKI (and its components), and Common Access Card (CAC) concepts. Lectures also include numerous links to additional information such as URL links that are external to this thesis that contain detailed concept information, term definitions, power-point slides and/or animations.

Another essential characteristic that must be taken into consideration during the design phase is a web-site's structure. Additionally, ease of use, consistent tutorials structure, and flexible navigation within the presented information must be incorporated in the DoD PKI and CAC instruction tool. In this way, a user can more easily navigate through the various web-based tutorials' pages, easily finding the desired information.

Finally, after the completion of the lecture material, users will be directed to the test page. Through this page they will be tested for the level of understanding and comprehension of the provided information.

Should the DoD PKI and CAC tutorial presented in this thesis not satisfy the DoD, it can at least serve as a preliminary prototype that can be revised to meet their needs.

3. Web Site Hierarchy

This section provides the architecture and specific design of the DoD PKI and CAC instruction tool.

The tutorial's interface begins with a "Home" page. On this page users can view a general description of what this tutorial provides. In addition, on this page there is an option to either "Log On" (for already existing users) or "Register" (for new users).

Once users have gone through a successful "Log On" process, they will be directed to the main navigation page--the Home Page. This page briefly describes the site, contains the main navigational functionality of the site and lists the overall point of contact for the site. Before starting the lecture pages, users will view a page which contains the navigational links for the lectures and information for each of them, within the site. Users are given the capability to access "Tests", complete "Evaluations", access a frequently asked question (FAQ) page, a "Feedback" page, a "Glossary" page, a "Help" page, a "Contact Us" page, a "Configuration Guides" page and finally a "Logoff" page (when a user selects the "Logoff" option, he/she has only two options; either of logging off the system or going back to the "Home" page). All of these links are accessible from the "HomePage" page (after a successful "Log On" or "Registration" process has been completed). Additionally, links to "Home", "Glossary" and "Help" pages are available directly from any of the lecture pages. Furthermore, users can view or download items and return to their previous page, at any time during their view or download session.

As for the layout and design of the pages, an effort was made to allow users to access the information desired with as few mouse clicks as possible.

Figure 17 illustrates a general diagram of the tutorial's interface pages:

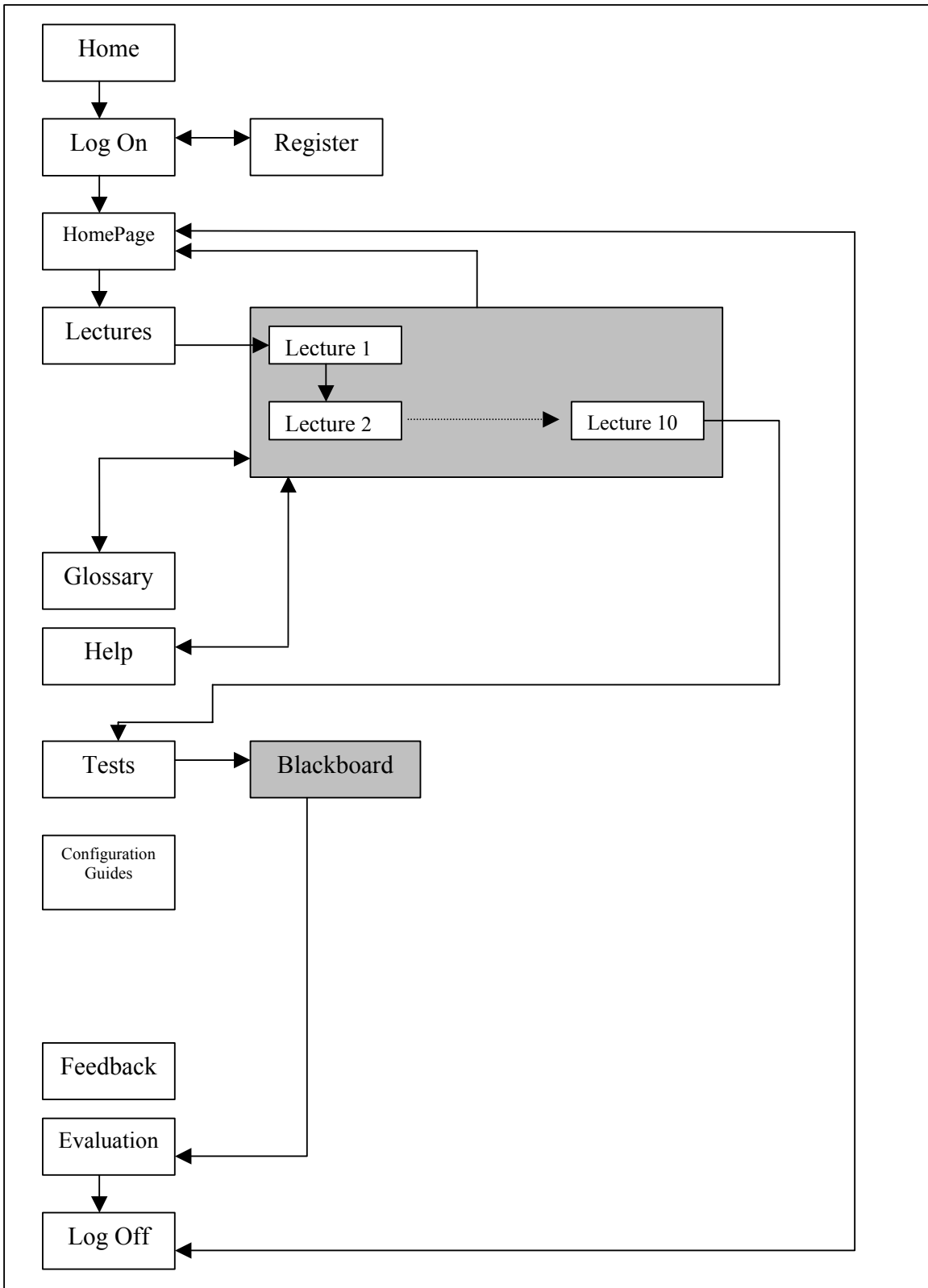


Figure 17. DoD PKI and CAC Tutorial's General Diagram

The site contains both HTML (hypertext mark-up language) and ASP (active server pages) pages. The HTML pages present basic text/photo information and navigational links. The ASP pages provide the link to the tutorial's databases (Log on, Evaluation, and Feedback). These pages provide result sets from information entered by users. The distinction between these pages is seamless to users, and contributes to better performance and functionality of the tutorial. The following Table 4 provides a list of all of the web-site's pages and their corresponding file names.

Page	file name
Login page	Default.htm
Home page	HomePage.htm
Registration page	RegistrationForm.asp
Registration Confirmation page	RegistrationConfirmation.htm
Log On page	LogOnForm.asp
Log On Confirmation page	LogOnConfirmationPage.asp
Log On Failure page	LogOnFailurePage.htm
Lectures page	Lectures Page.htm
Cryptography page	Cryptography.htm
Symmetric Cryptography page	Secret Key Cryptography.htm
Public key cryptography page	PublicKeyCryptography.htm
Public key cryptography (cont.) page	PublicKeyCryptography_2.htm
Digital Signature page	DigitalSignature.htm
Digital Certificates page	Certificates.htm
Digital Certificates (cont.) page	Certificates_2.htm
Certification Authority page	Certification Authority.htm
Certificate Verification page	CertificateVerification.htm
Revocation page	Revocation.htm
Root Certificate Authority page	RootCA.htm
Introduction To PKI page	IntroductionTo PKI.htm
PKI Components page	PkiComponents.htm
Common Access Card (CAC) Introduction page	CACIntroduction.htm
Common Access Card (CAC) (cont.) page	CAC_2.htm
Common Access Card (CAC) (cont.) page	CAC_2A.htm
Common Access Card (CAC) (cont.) page	CAC_3.htm
Common Access Card (CAC) (cont.) page	CAC_4.htm
Glossary page	Glossary.htm
FAQ page	Frequently Asked Questions.htm
External links page	External_links.htm
Contact Us page	contact.htm
Feedback page	FeedbackForm.asp
Help page	help.htm
Log Off page	Log Off Form.htm
Log Off Confirmation page	LogOffConfirmationPage.htm
Website Evaluation page	Evaluation.asp
Configuration Guides page	ConfigurationGuides.htm
Global Directory Services (GDS) page	GLOBAL_DIRECTORY_SERVICES.htm

Table 4. DoD PKI and CAC Tutorial Pages

The Web-site utilizes a standard font and color scheme to ensure consistency throughout all of its pages. The exception to this will be the evaluation part, which is implemented through the Blackboard application. The evaluations were implemented on Blackboard as it contained the functionality necessary to achieve randomly generated quizzes from the total list of questions provided. Furthermore, this site incorporates various formats of training information, such as PowerPoint slides and short Flash animations.

The Appendix includes screen shots of several of the central pages that comprise the core content of the tutorial.

4. Tutorial's Database Sketch

This section presents the design details of the DoD PKI and CAC training databases. The tutorial includes three databases, which meet the described functional requirements and contribute to its performance and functionality.

The tutorial's databases collect user-associated information that can be used for further improvement of the tutorial. This includes each user's identifying information, the feedback form, and the evaluation form. Also, information about user test results is maintained in the Blackboard grade book.

All the information collected from the databases can be useful for future improvements/modifications of the DoD PKI and CAC training instruction tool.

5. Tutorial's Maintenance and Control

Currently, DoD PKI user training is not centrally controlled, but rather it is dispersed throughout its departments and commands. Because of this, common training and material updates are not ensured for all the DoD users. In order to ensure that the most up-to-date training is presented, and that all users have access to the same training, the content of the DoD PKI and CAC instruction tool should be centrally controlled and maintained.

6. Tracking the Training

The PKI and CAC instruction tool is designed to support the tracking of user training. This tracking functionality is built into the tutorial through features that are provided by Blackboard. The Blackboard training database contains a record, called 'Grade book' which contains information about users and their performance. After completing a test session, the results are stored in this record and can be viewed by the instructor or system administrator. Further use of the collected results can be processed in order to contribute to improvements of the tutorial. Additionally, concern must be taken for the security of each user's personal data, due to the fact that collected records identify users and their test results. This collected evaluation information personal data and training can be integrated at the DoD level to ensure that appropriate training is being completed by end users throughout the DoD.

Web-based training has been shown to be an efficient, effective method of delivery in environments such as DoD. The DoD PKI and CAC tutorial can offer the basic structure within which DoD PKI and CAC training can be housed and distributed to those who need it.

VI. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

The scope of this thesis was the development a user-friendly, web-based, instruction and training tool about PKI and CAC concepts and technologies. When this effort was started, there were several concerns to bear in mind. Those were: learning how to instruct, learning how to apply already existing instructional practices to a new environment (i.e., the Web), and designing a tutorial that was interesting, accurate and didactically efficient learning experience.

Due to the particularities concerning teaching technical subjects to military personnel, the author believes that his research in the area of instructional design and practices provided the opportunity to at least construct an interesting tutorial delivery. As for the second factor (interesting), efforts were concentrated on combining various media that would make the learning experience more attractive. An attempt was made to create a more understandable and user-friendly instruction tool using these components. Hopefully, by collecting the results of the evaluation form/surveys that the trainees will submit, it will be possible to have the opportunity to learn much from their comments and suggestions, and perhaps make additional improvements.

This thesis presented a DoD PKI and CAC instruction tool implemented in a Web-based format. Web-based instruction benefits from the wide accessibility of the Web to make training time and place independent. Web-based instruction can perform a supplementary role to traditional classroom instruction. Within the DoD environment, Web-based instruction is an ideal solution for service men and women with time and place constraints. In addition, this new environment offers some useful pedagogic delivery tools, including: discussion forums, multi-media components, animations and simulations, all of which combine to provide a more intuitive clarification of complex concepts.

A Public Key Infrastructure by itself is a complex combination of computer and cryptographic technologies. When attempting to adapt these technologies to the specific policy requirements of a large organization (e.g., the U.S. DoD), additional complication

and/or confusion related to the infrastructure's correct implementation is added. Given the importance of user understanding to the successful implementation of a PKI, the use of this tutorial should help address DoD PKI user understanding of the CAC element of the overall infrastructure.

This thesis attempted to determine and summarize the larger DoD PKI environment and all the essential elements of DoD PKI that all CAC card users should be knowledgeable of. It provides a basic overview of the PKI and CAC. It has an implemented test and test evaluation functionality through Blackboard, that stores the test results and provides the users with a pass or fail message.

This Web-based instruction tool is only the start of what is needed in order to make this instruction tool ready for adoption within the DoD environment. Further testing of this tutorial is necessary to identify any possible subject matter or user interface deficiencies.

Another requirement that must be met is the tutorial's capability for more customizable training to meet the different needs of the various DoD services and commands, and address any new PKI-enabled applications as they become available. One of this tutorial's advantages is its hyper-linking flexibility which provides the capability of extending it as new material is offered.

Additional issues concerning the tutorial may include the creation of user profiles to support record-keeping for related training that may occur over the course of a person's career.

Finally, the DoD PKI and CAC Web-based tutorial establishes a groundwork for continuous research in the region of distance training. The novel ideas in this area have to do with the advancement of software and training equipment. Hopefully, many of the problems encountered during the development of this web-based tutorial will be solved in the near future due the new technology improvements and innovations.

B. FUTURE WORK

In addition to the delivered DoD PKI and CAC web-based instruction tool, associated issues exist that, with further investigation, could provide added benefits to DoD. Some of these possible areas of research are:

- The tool's integration to incorporate information for other more detailed and specific training based on the specific assigned duties of each user.
- Incorporation of training for new PKI-enabled applications that are adopted and implemented by the DoD. Owing to the extensibility provided by the hyperlinked and modular structure of this tutorial, this task should be relatively easy to do.
- Incorporation of training for new applets that are Command customized.
- Testing of the instruction tool for perceived training value and ease of use and study of the evaluation survey forms. Thus, any missing or misleading information will be identified and the necessary modifications will be made.
- Construction and maintenance of a detailed "Troubleshooting" page, in order to provide users facing problems with information and specific instructions.
- Incorporation and adoption of user identification procedures in order to access more classified information, based on a user's clearance and organization's security policies and restrictions.
- Development and integration of a mechanism that will keep track of a user's training based upon command assignments.
- Development and integration of a mechanism that will not allow users to perform any action within the DoD PKI environment except authentication, unless a minimal training process has been completed.
- Identification of the appropriate remediation procedure for test failures (i.e., retaking training requirements).
- Identification of the appropriate mechanism by which notification of successful test completion can be communicated to a specified database server (i.e., a test taker's supporting Personnel Administration office?).

As indicated previously, this thesis work was to design, construct and implement a DoD PKI and CAC web-based instruction tool. All the aforementioned issues are additional aspects of training elements that could improve upon this tutorial. Although the need for conventional education (classroom) is not likely to go away, this tutorial will contribute to the integration of training efforts directed at the DoD PKI.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. INSTRUCTION TOOL SCREENSHOTS

Some screenshots of the web-based instruction tool are provided (a sample of this work). Hopefully they would be helpful to the reader to understand some of the project issues. Because the website has a dynamic structure its full capabilities can be presented and tested only through the web.



Figure 18. Login Screen

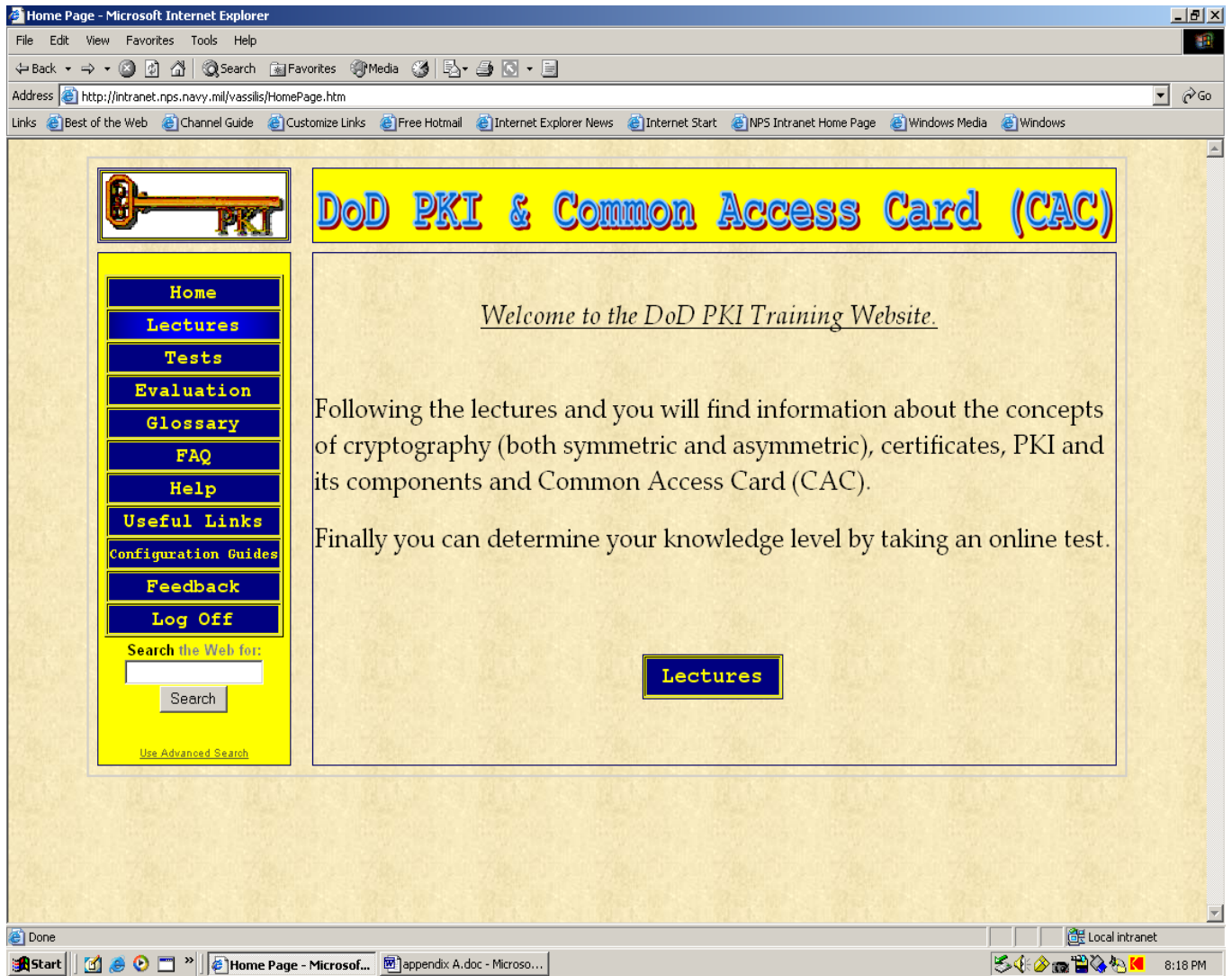


Figure 19. Home Page

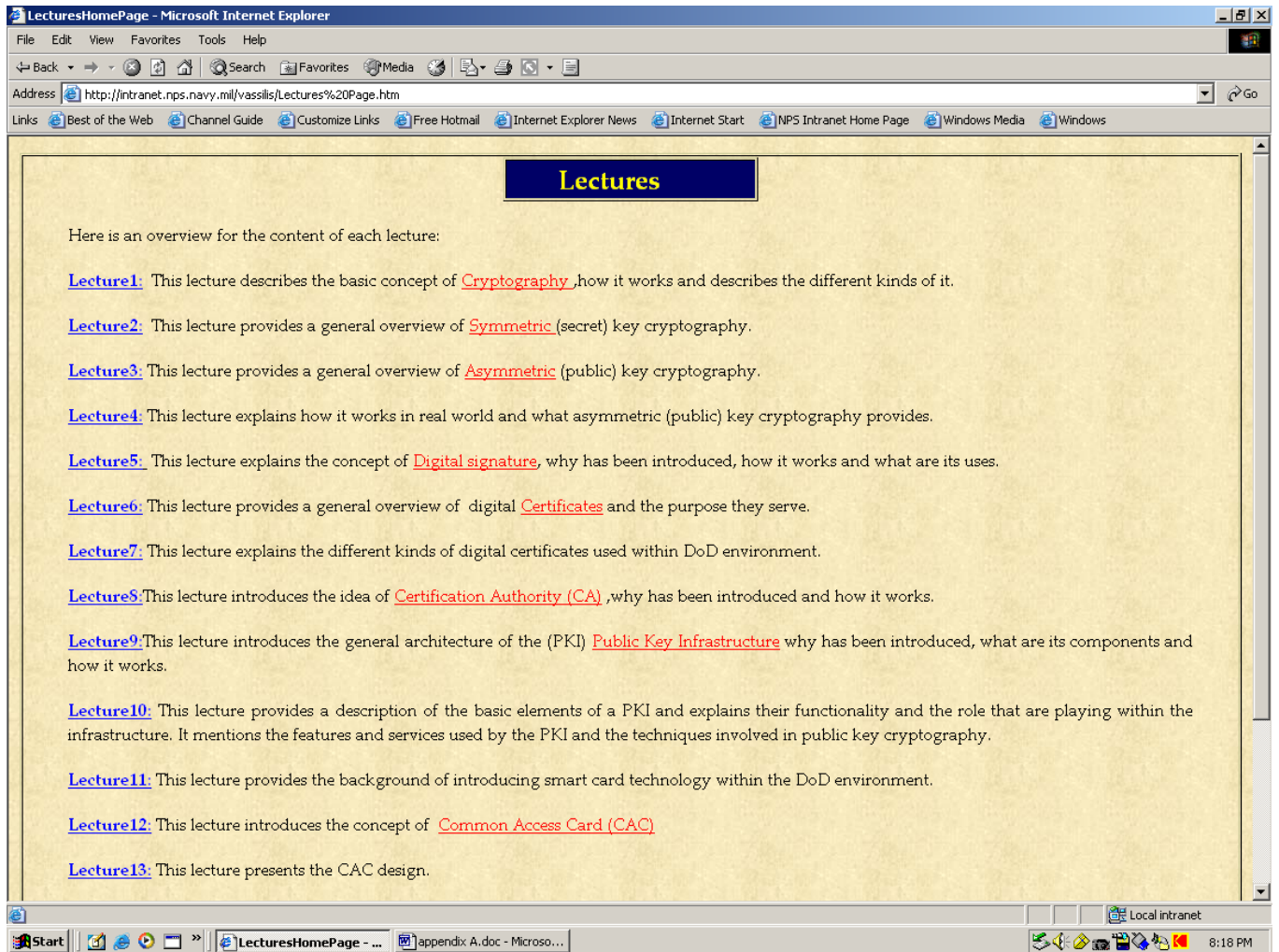


Figure 20. Lectures Contents

http://intranet.nps.navy.mil/vassilis/Secret Key Cryptography.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://intranet.nps.navy.mil/vassilis/Secret%20Key%20Cryptography.htm

Links Best of the Web Channel Guide Customize Links Free Hotmail Internet Explorer News Internet Start NPS Intranet Home Page Windows Media Windows

Secret (symmetric) Key Cryptography

Also called conventional cryptography utilizes one key (the same key, called [secret key](#)) - for both encryption and decryption - of a message. This key is used from the sender to encrypt data to ciphertext and then from the recipient to decrypt ciphertext (encrypted data) to plaintext again.

The security of the encrypted data depends upon the strength of both the key and the encryption algorithm. The system's security relies on two factors: *how strong is the secret key* and *which algorithm is used for encryption*.

Symmetric Key Cryptography is simple, fast and secure under one condition: secret key must always be kept safe.

So, if we want to implement symmetric cryptography, what we need is:

1. all users must have a copy of the key and
2. confidentiality of the key must be assured

```

graph LR
    Alice[Alice] -- "This is a clear text message" --> Encrypt[Encrypt]
    Key1[Key] --> Encrypt
    Encrypt -- "qANQRIDB  
wU4DVuK5  
K!cgm7wQ  
B!9yPZ5+" --> Encrypted[Encrypted Message]
    Encrypted --> Decrypt[Decrypt]
    Key2[Key] --> Decrypt
    Decrypt -- "This is a clear text message" --> Bob[Bob]
  
```

Done

Start | LecturesHomePage - Micr... | http://intranet.nps.na... | Local intranet | 8:01 PM

Figure 21. Secret Key Cryptography Introduction

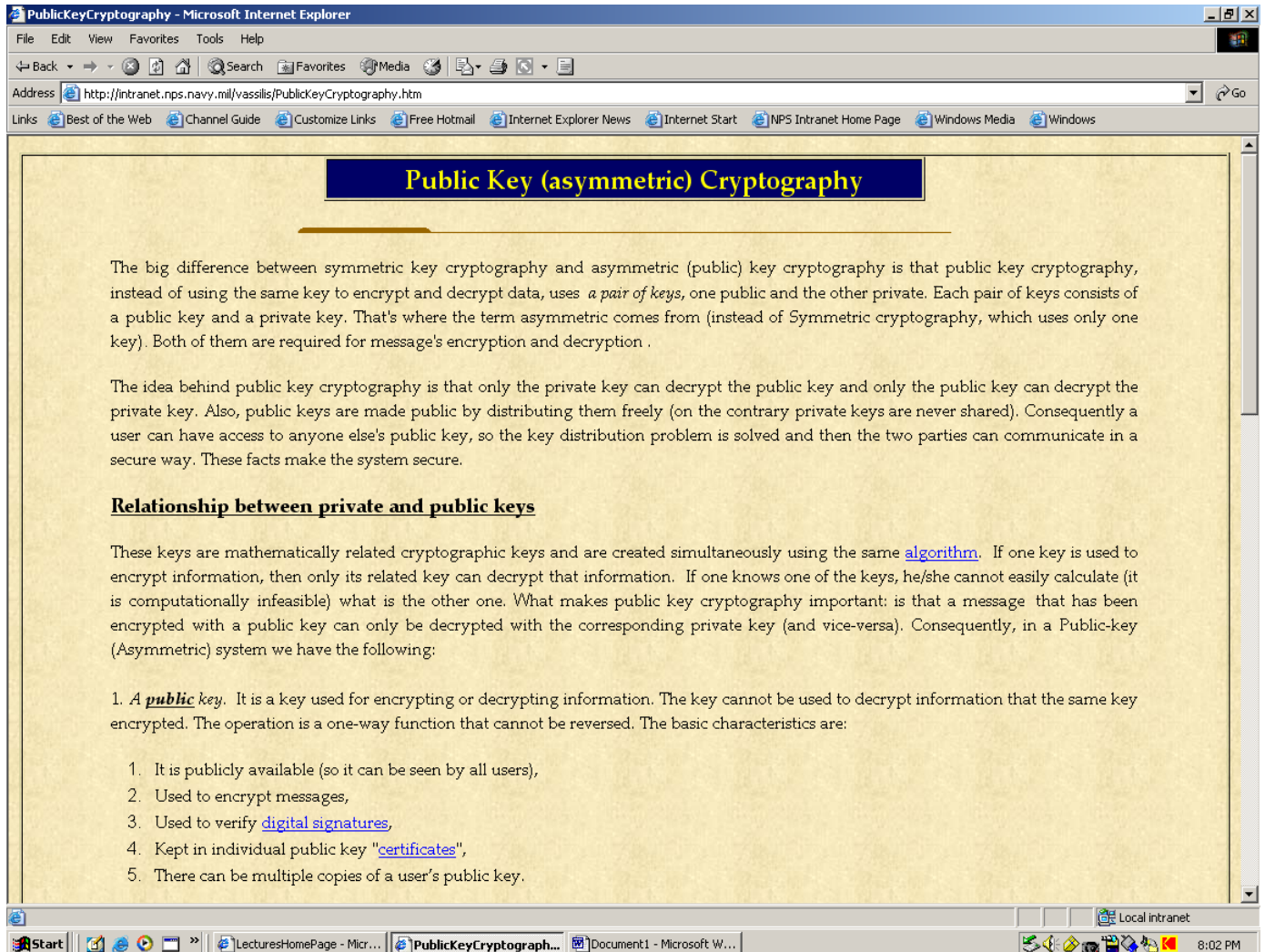


Figure 22. Public Key Cryptography Introduction

Public key cryptography (cont.)

In normal practice, both symmetric and asymmetric cryptographic mechanisms are used together in order to achieve both stronger security and to take advantage of the strengths of each; that is, the ability to distribute public keys without concern for their confidentiality (the strength of asymmetric key cryptography), and the faster encryption/decryption speed of secret keys (the strength of symmetric key cryptography). The general usage then is to use an asymmetric mechanism to securely deliver a secret key, then to have the actual information being sent encrypted using the secret key. This secret key can be any sufficiently long random number. And since the general usage is to generate at least one new secret key for each session of communication between two parties, the secret key is often also referred to as the session key. The public key is used to encrypt the session key and both the session key and the information encrypted with it are sent to the recipient. The recipient will use her private key to decrypt the session key, and then use it to decrypt the actual information. This is much faster than using the private key to decrypt all of the information. The following figure illustrates this practice:

The diagram illustrates the process of public key cryptography between Alice and Bob. Alice starts by generating a session key and encrypting her message with it. She then encrypts the session key using Bob's public key. Both the encrypted session key and the encrypted message are sent to Bob. Bob uses his private key to decrypt the session key and then uses the session key to decrypt the message.

Alice's actions:

- 1) Generates session key
- 2) Encrypts message with session key
- 3) Encrypts session key with Bob's public key

Bob's actions:

- 1) Decrypts session key with his private key.
- 2) Decrypts message with session key

The diagram shows the flow of data: Alice's message is encrypted with a session key to create an encrypted message. The session key is then encrypted with Bob's public key. Both the encrypted session key and the encrypted message are sent to Bob. Bob uses his private key to decrypt the session key, and then uses the session key to decrypt the message.

Figure 23. Public Key Cryptography (cont.)

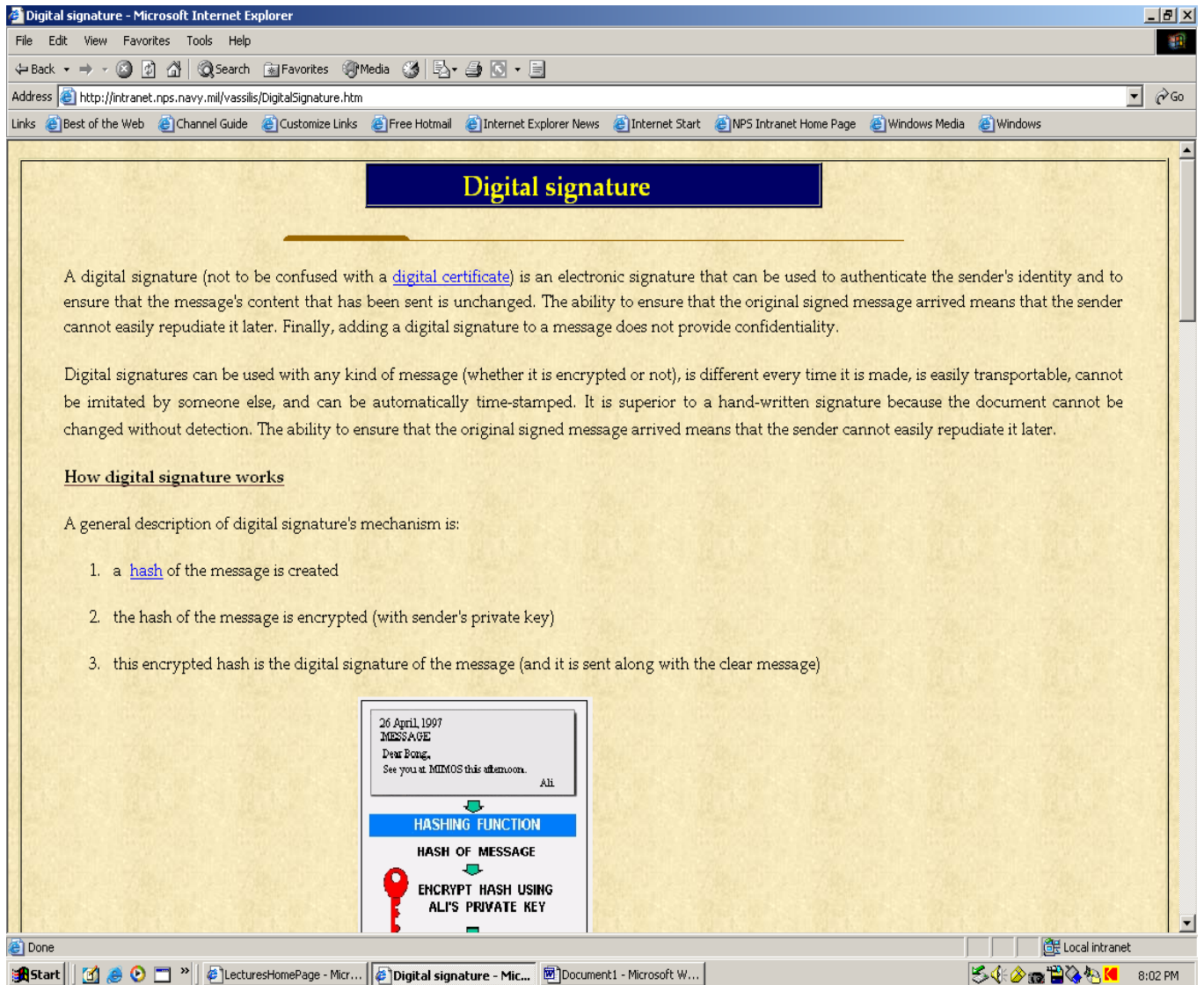


Figure 24. Digital Signature

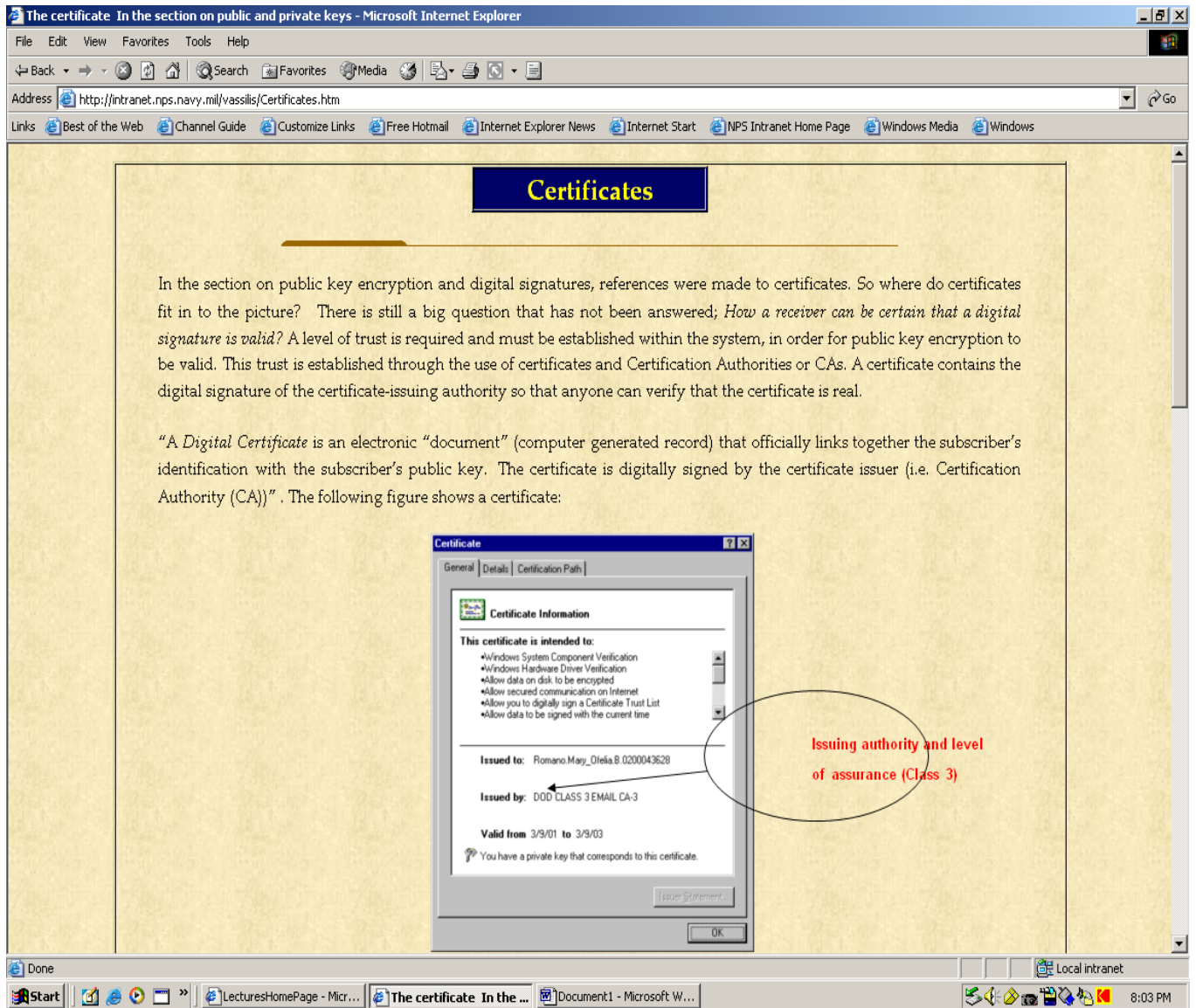


Figure 25. Certificates

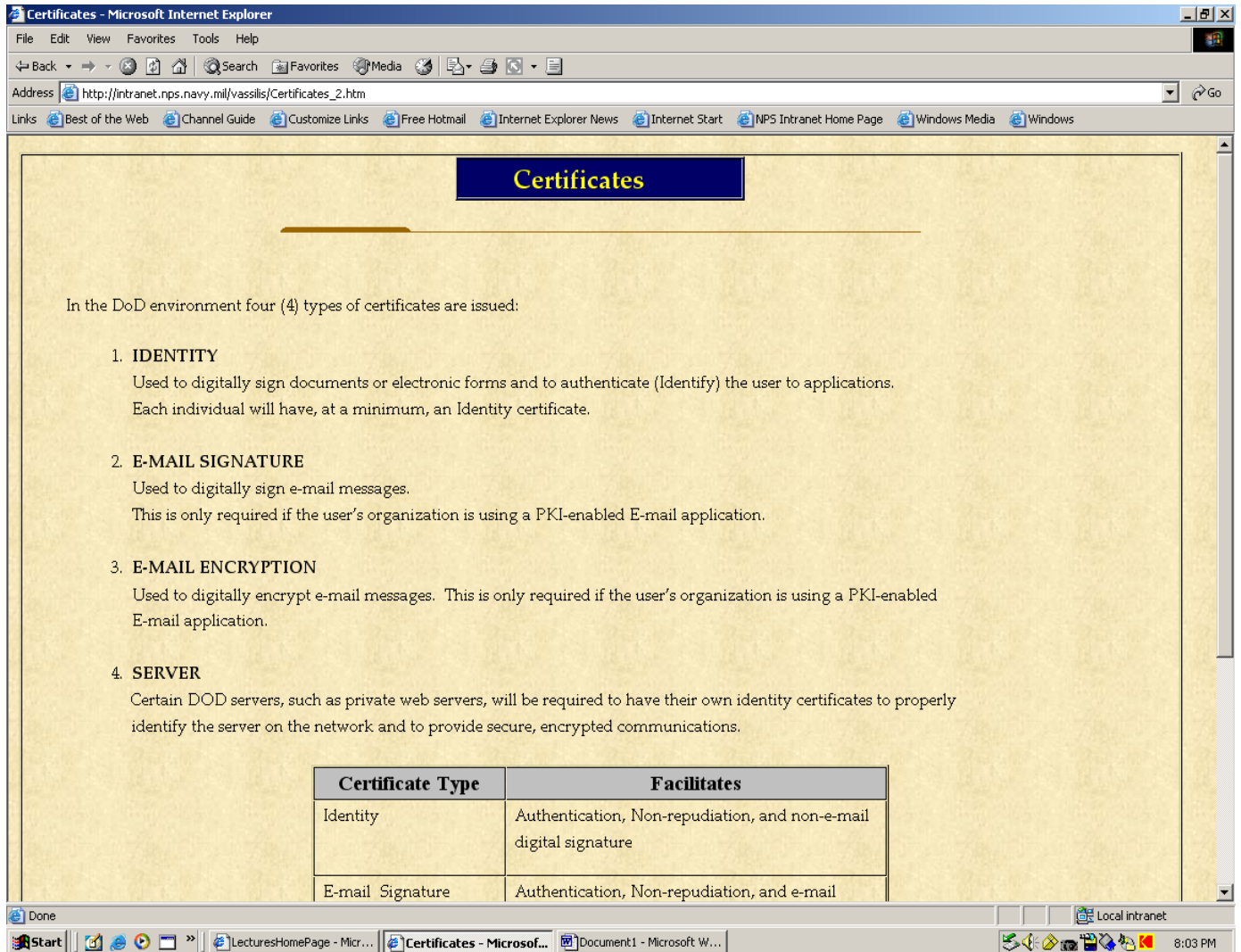


Figure 26. Types of Certificates

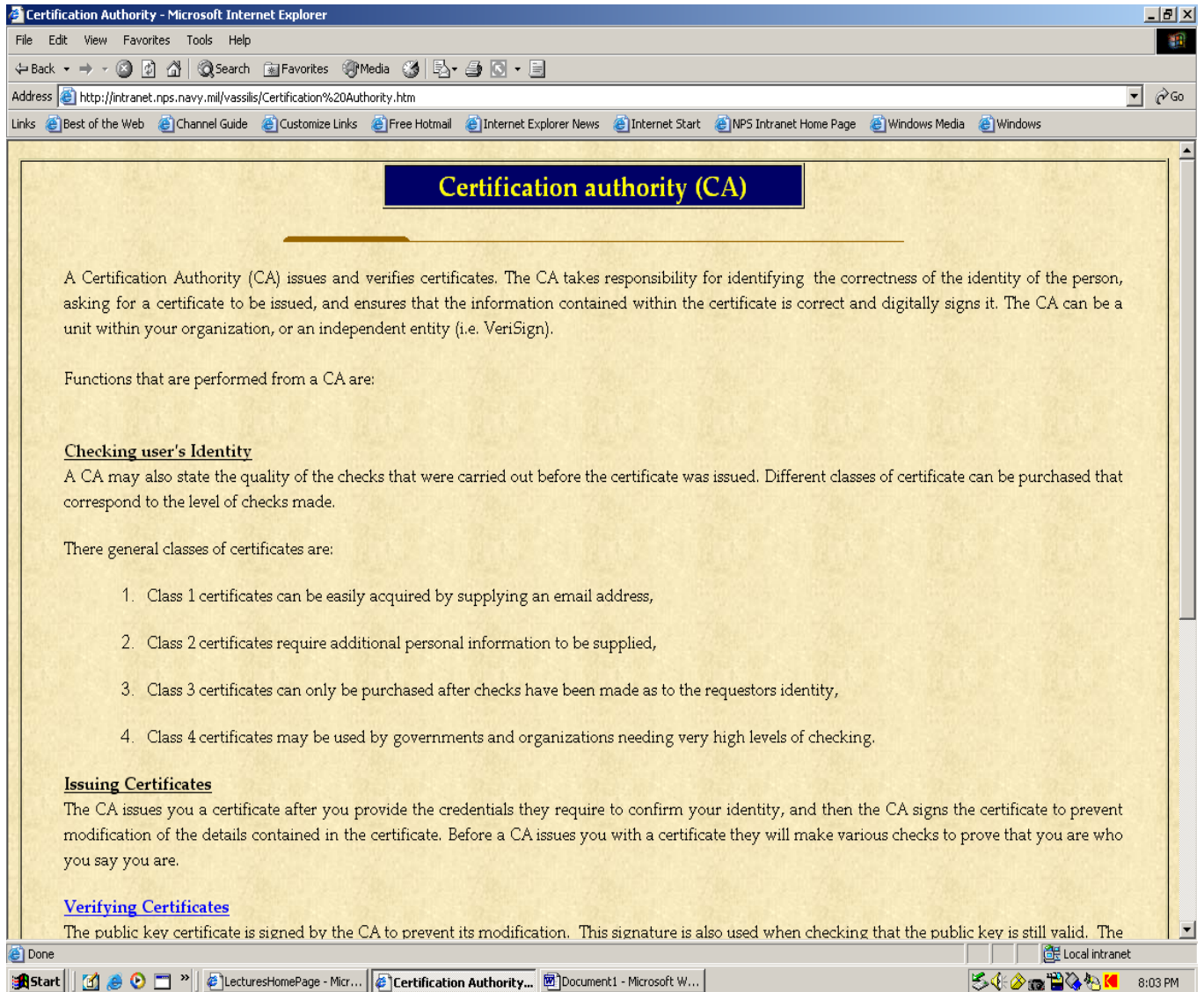


Figure 27. Certification Authority

http://intranet.nps.navy.mil/vassilis/CertificateVerification.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

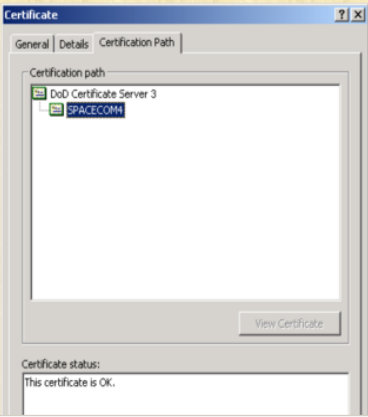
Address http://intranet.nps.navy.mil/vassilis/CertificateVerification.htm

Links Best of the Web Channel Guide Customize Links Free Hotmail Internet Explorer News Internet Start NPS Intranet Home Page Windows Media Windows

Verifying Certificates

It is already known that a user's public key certificate - in order its modification to be prevented - is digitally signed by the CA. *This signature is also used when checking that the public key is still valid.* The signature is validated against a list of Root CAs contained within various PKI aware applications (e.g. your browser). Some CA certificates are called [Root Certificates](#) as they form the root of all certificate validation. Certificate validation occurs automatically using the appropriate public certificate contained within the root CA list. Also, **in order a certificate to be valid, every certificate within that certificate chain must also be valid.** On the following figures we can see an example of a certificate chain in a Microsoft Windows 2000 network.

1. The certificate was issued by SPACECOM4, a subordinate CA.
2. SPACECOM4 is signed by the root CA, DoD Certificate Server 3.



Certificate

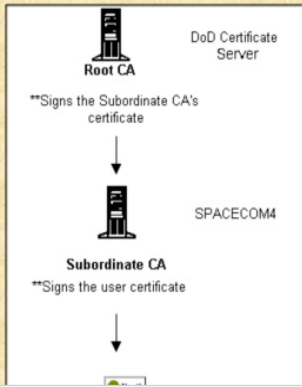
General Details Certification Path

Certification path

- DoD Certificate Server 3
- SPACECOM4

View Certificate

Certificate status:
This certificate is OK.



DoD Certificate Server

Root CA

**Signs the Subordinate CA's certificate

↓

SPACECOM4

Subordinate CA

**Signs the user certificate

↓

Done

Start | LecturesHomePage - Mic... | http://intranet.nps.na... | Document1 - Microsoft W... | Local intranet | 8:04 PM

Figure 28. Certificate Verification

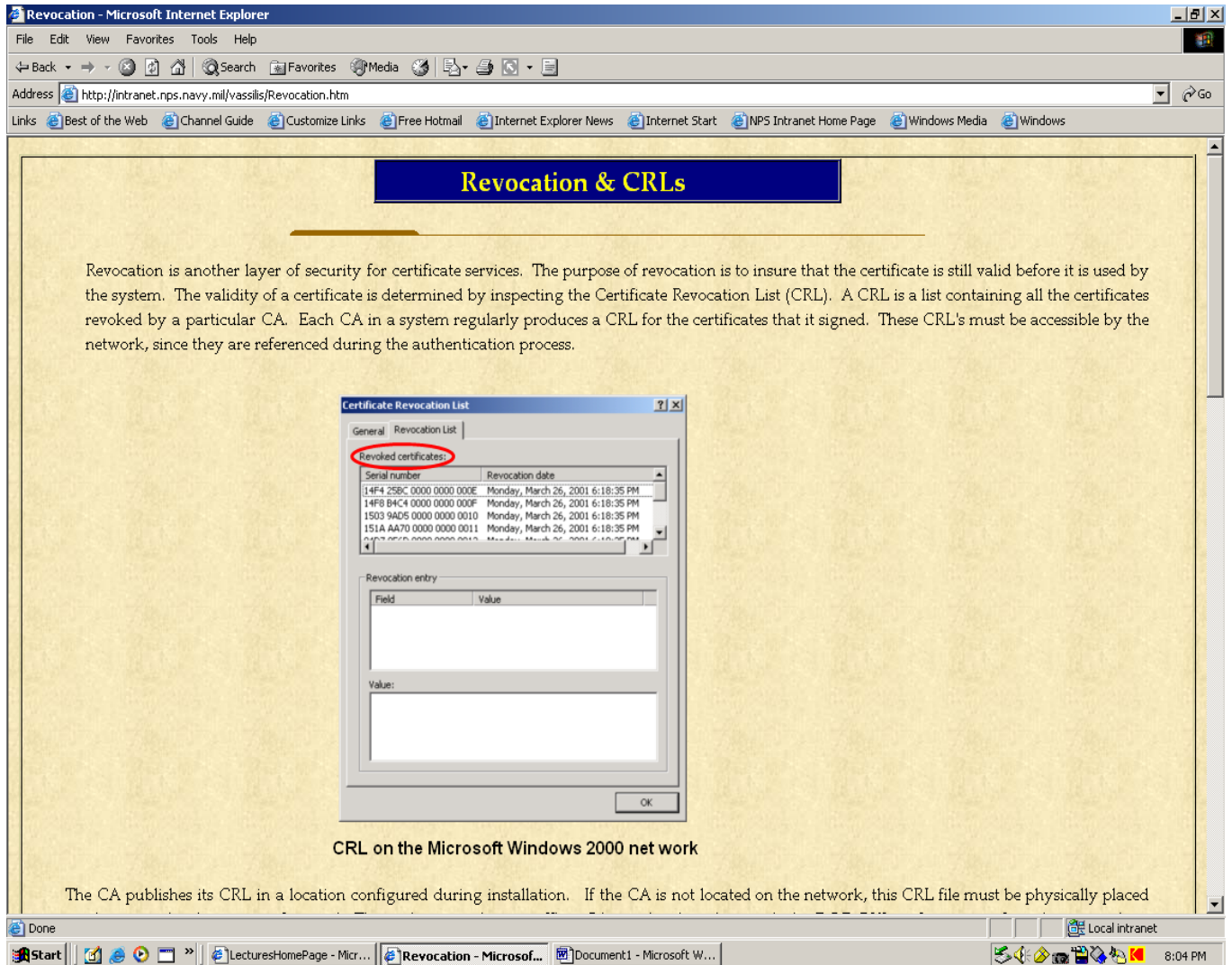


Figure 29. Certificate Revocation List (CRL)

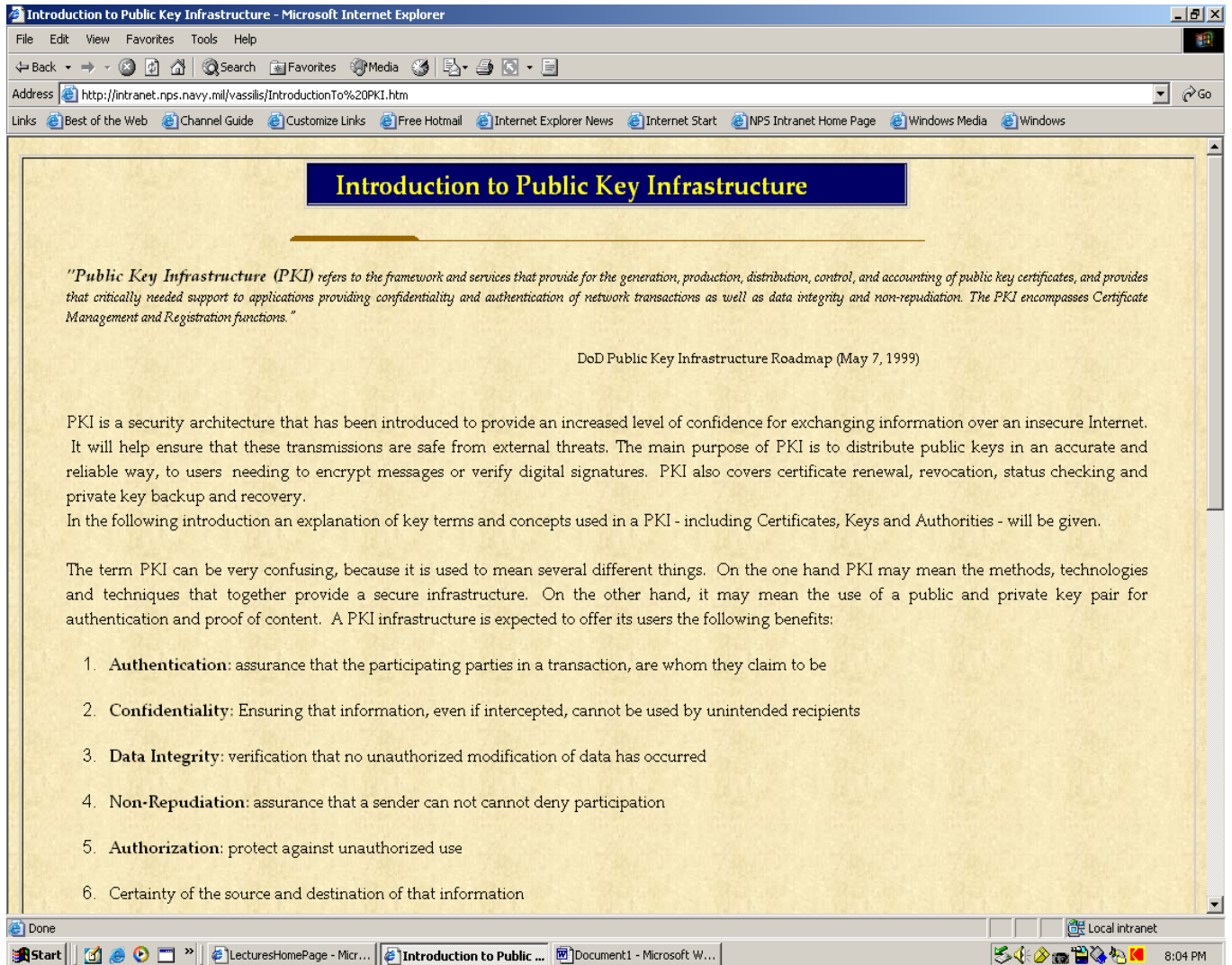


Figure 30. Introduction to Public Key Infrastructure

Public Key Infrastructure (PKI) Components

A PKI is made by combining a number of services and technologies. These elements (either hardware elements or software processes) are:

1. Root Certification Authority (Root CA)
2. Certification Authority (CA)
3. Registration Authority (RA)
4. Local Registration Authority (LRA)
5. Directories
6. Users
7. Relying Parties

These elements are linked together as seen in the following figure:

The diagram illustrates the PKI components and their interactions. At the top is the **Root CA**. Below it is the **Certification Authority (CA)**. To the right is the **Registration** component, which includes sub-functions: *Establish LRAs,* *Revoke Certificates,* and *Process Server Certificates*. Below the CA is the **Local Registration Authority**. To the left is the **Certificate Directory**. The interactions are as follows:

- A solid line connects the **Root CA** to the **Certification Authority (CA)**.
- A solid line connects the **Certification Authority (CA)** to the **Local Registration Authority**.
- A solid line connects the **Local Registration Authority** to the **Registration** component.
- A solid line connects the **Registration** component to the **Certification Authority (CA)**.
- A solid line connects the **Certification Authority (CA)** to the **Certificate Directory**.
- A solid line connects the **Certificate Directory** to the **Certification Authority (CA)**.
- A dashed line connects the **Registration** component to the **Root CA**.
- Labels on the diagram include: *Certificate Publish* (from CA to Directory), *Certificate* (from Directory to CA), *Certificate Download* (from CA to LRA), and *Certificate* (from LRA to CA).

Figure 31. PKI Components

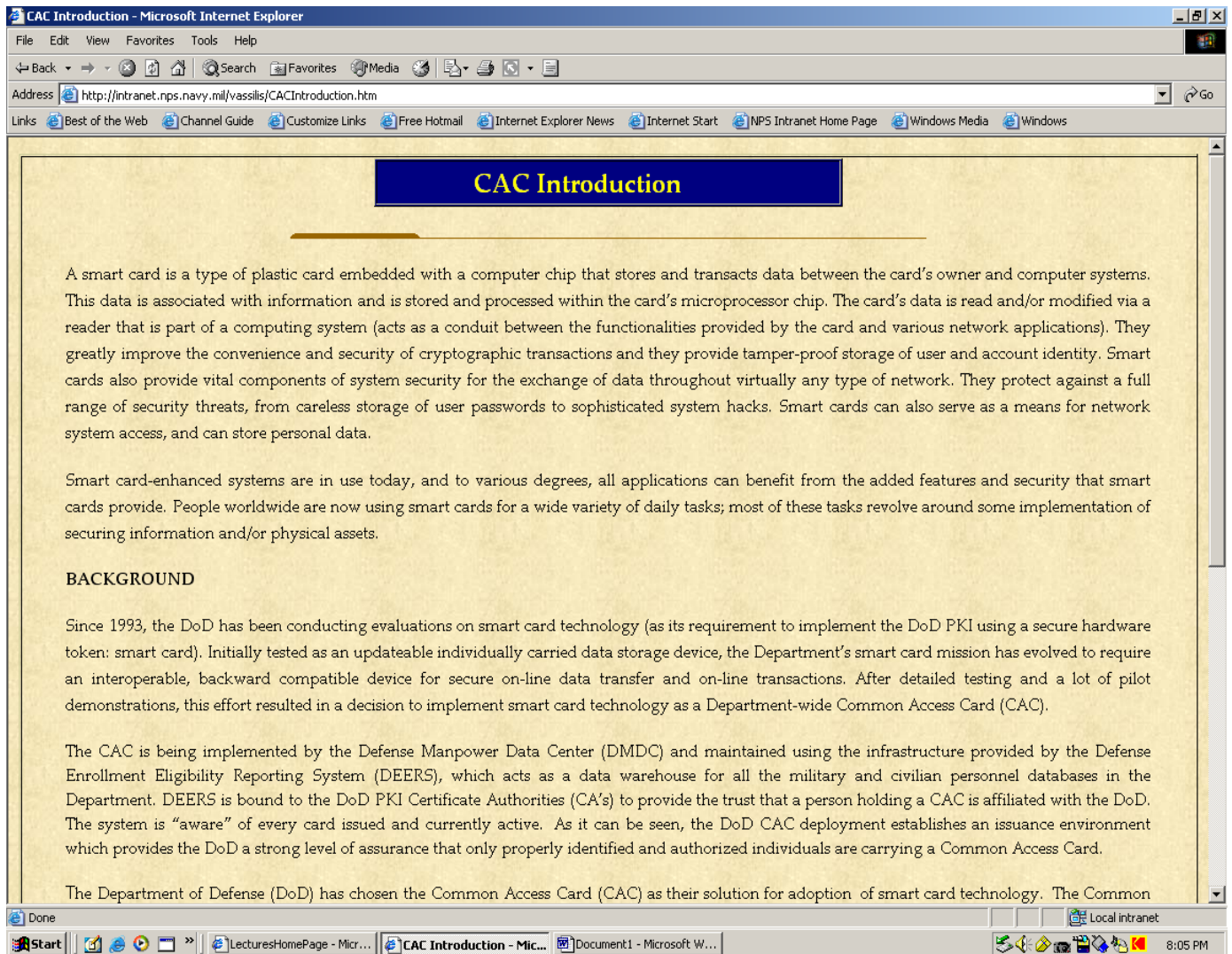


Figure 32. CAC Introduction

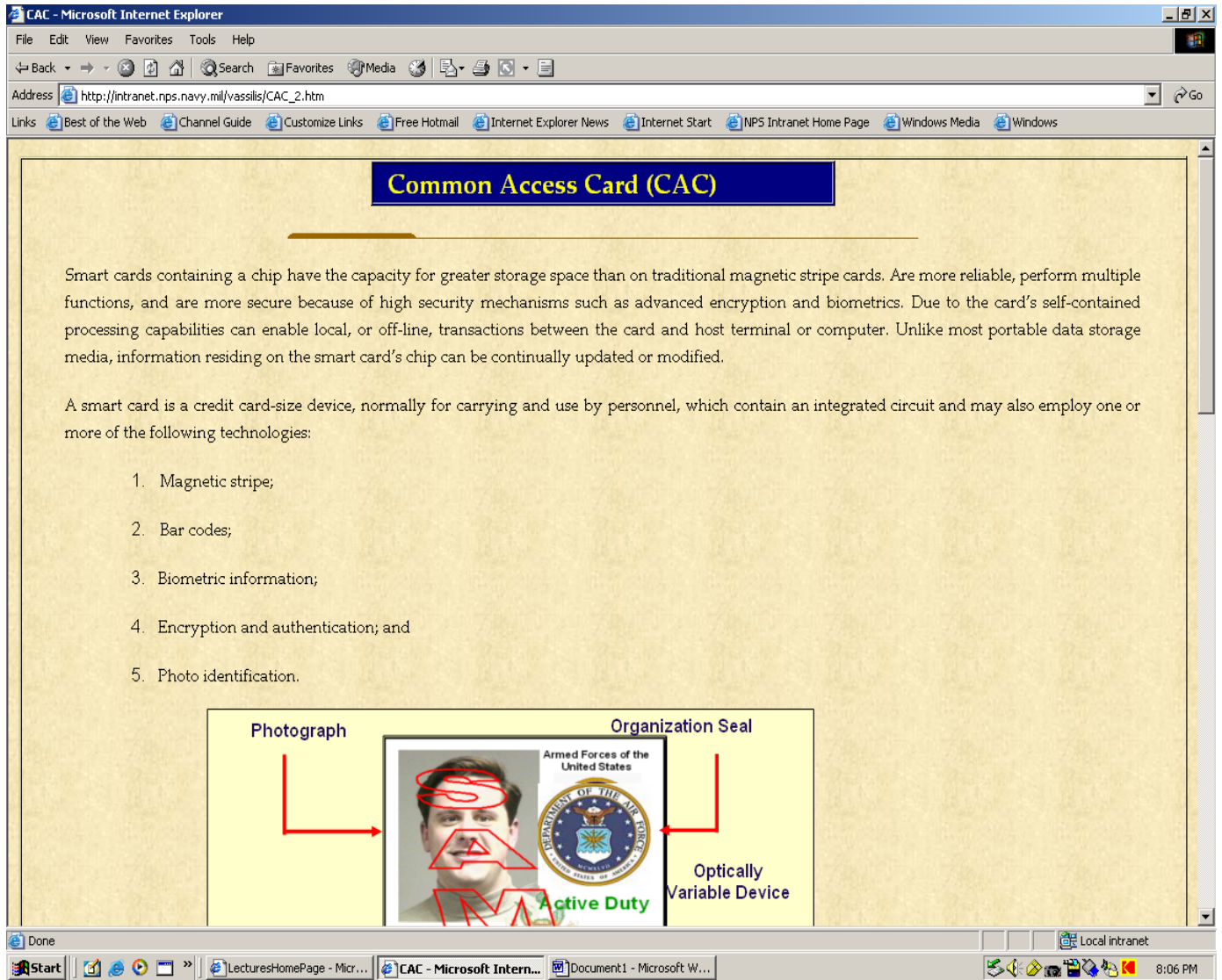


Figure 33. Common Access Card (CAC)

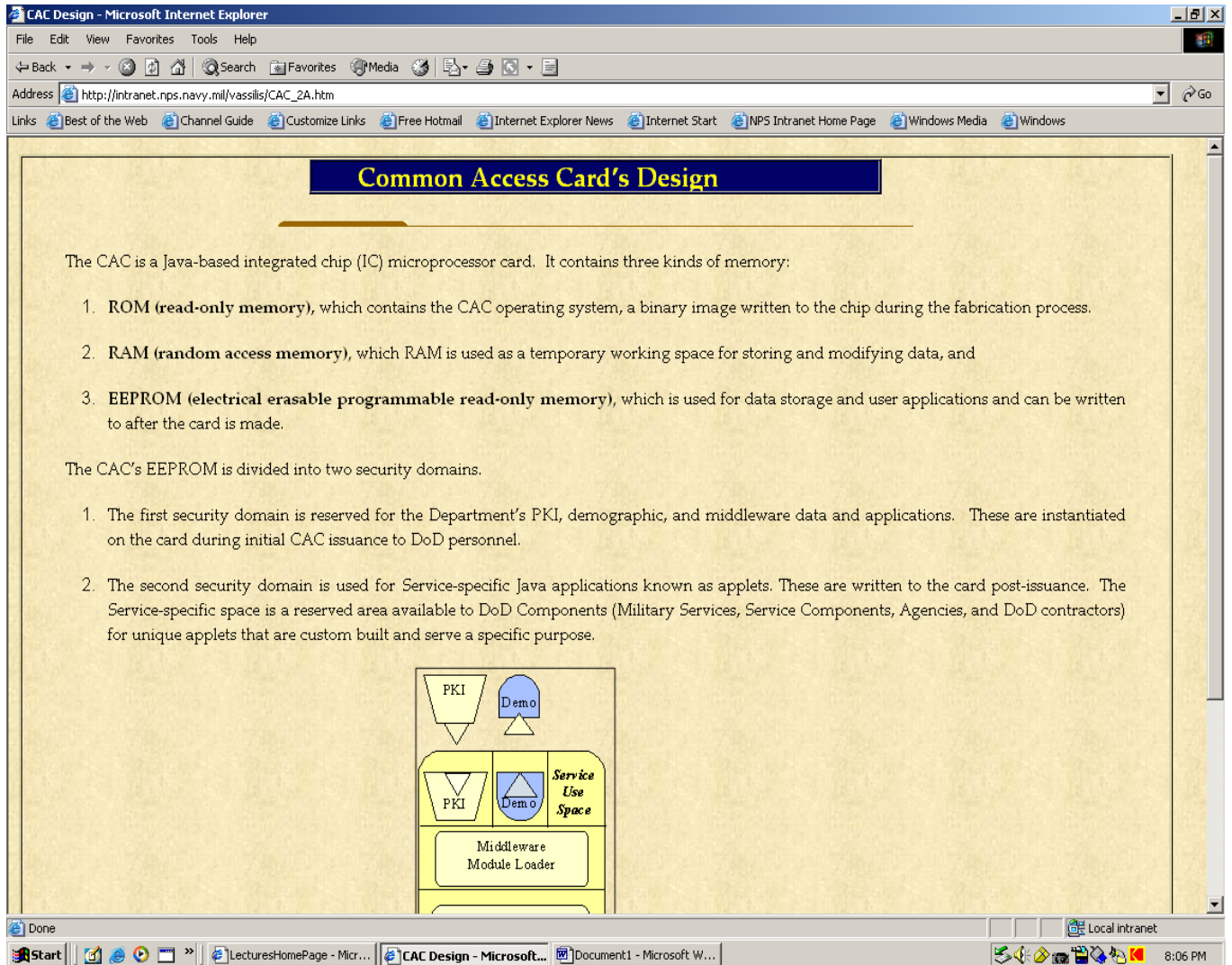


Figure 34. Common Access Card's Design

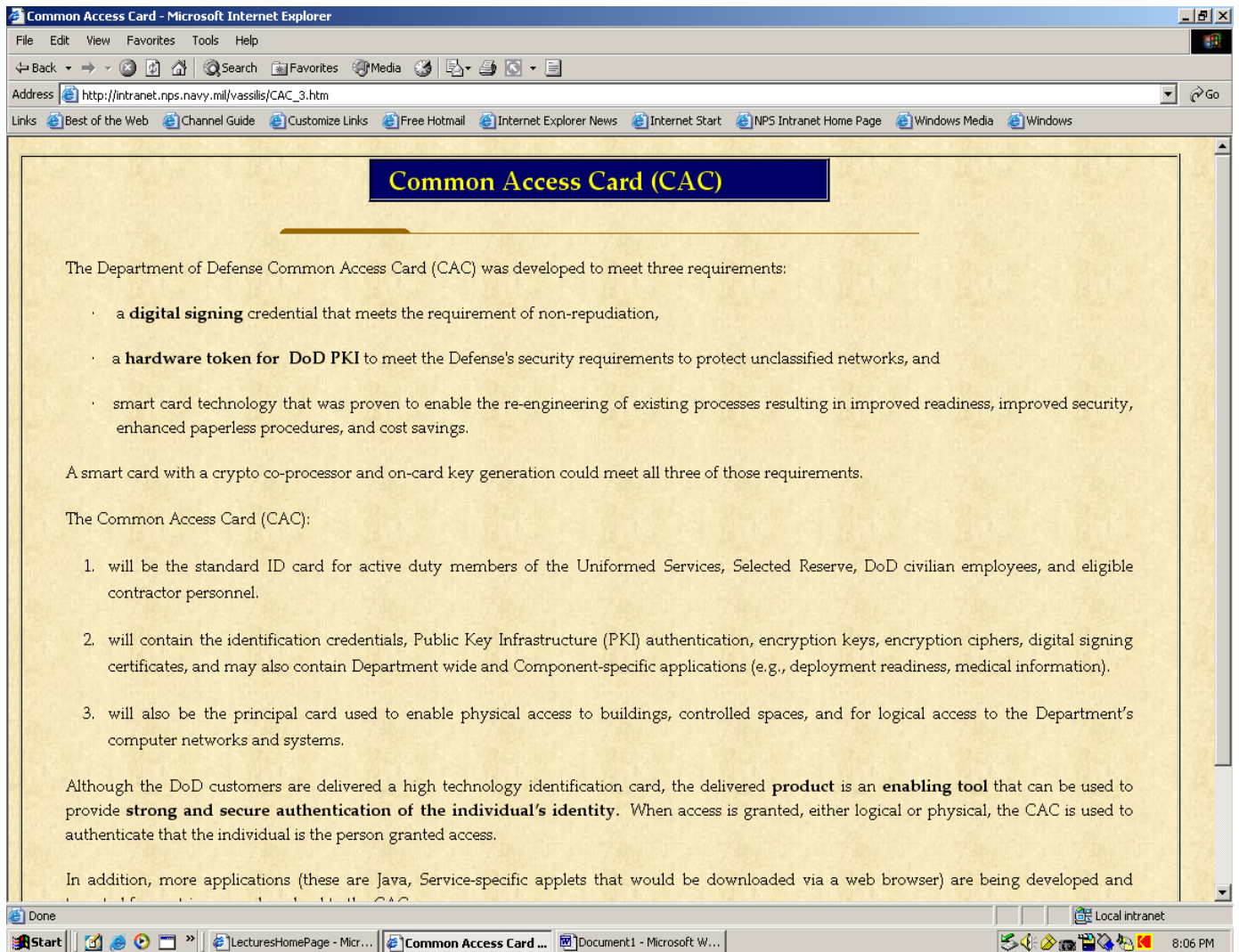


Figure 35. Common Access Card & DoD

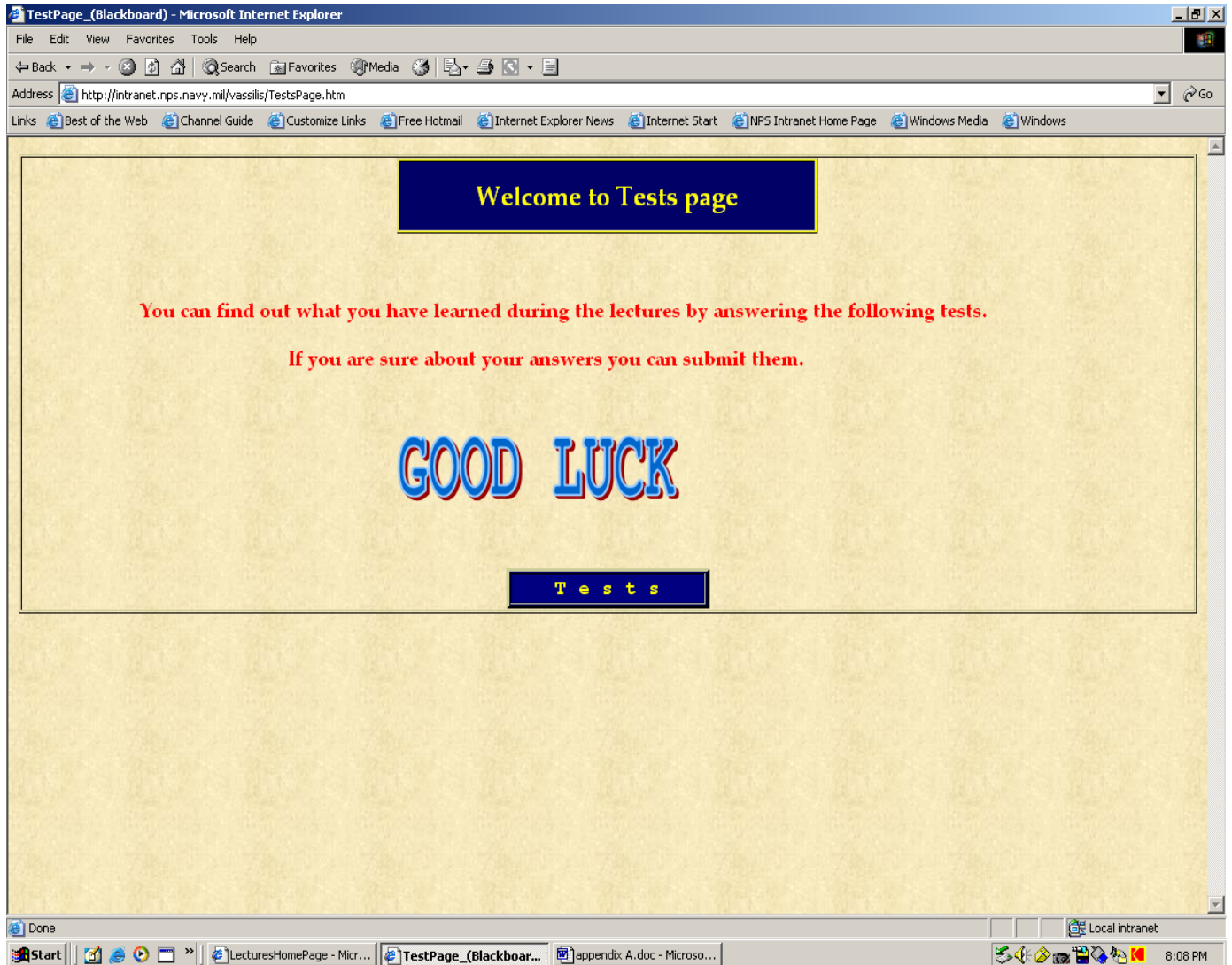


Figure 37. Test Page

LIST OF REFERENCES

1. "DoD Public Key Infrastructure", 5/22/2001, SPAWARSYSCEN Charleston, SPAWAR_pki_101.ppt.
2. Hale, R., and Friedrichs, P., "Public Key Infrastructure (PKI) and the Use of Cryptography for Automating and Securing DoD Business Processes," [<http://www.knowledgenet.mil/knet/Feb00/Feb00.pdf>, 28 January 2000] Accessed March 2004.
3. "Introduction to Public-Key Infrastructure," [<http://www.iplanet.com/developer/docs/articles/security/pki.html>] Accessed March 2004.
4. "DoD Medium Assurance Public Key Infrastructure CONOPS", 24 December 1997, conops-b.ppt.
5. Morris, D., "Public Key Infrastructure (PKI) Overview," 2001, morrisde@hqmc.usmc.mil.
6. Assistant Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12 August 2002, [<http://www.c3i.osd.mil/org/sio.ia/pki>] Accessed March 2004.
7. [<http://www.artisoft.com/pki.htm?OVRAW=digital%20signature&OVKEY=digital%20signature&OVMTC=standard>] Accessed March 2004.
8. DoD Public Key Infrastructure Program Management Office, "Public Key Infrastructure Roadmap for the Department of Defense, Version 3.0," 29 October 1999.
9. Austin, T., *PKI: A Wiley Tech Brief*, John Wiley & Sons, Inc., New York, New York, 2001.
10. IBM TP T20-23 - February 02 , SPAWAR, "*PKI Basics_June 2003*", PKI User's Conference [20 June 2003], 27 January 2003.
11. "Implementation of DoD Public Key Infrastructure", Air Force PKI SPO ESC/DIWS, 22 February 1999, CAC_Theatre_Tng_032202ses.ppt.
12. Hale, R., "Introduction to Public Key Infrastructure and Applications," 7 May 1999, [<http://falcon3.ncr.disa.mil/Pki.pdf>] Accessed March 2004.
13. Rod Stuhlmuller, 10/20/1999, "CAC The Common Access Card DMDC-Feb 2001", JPAS DMDC Brief.ppt.

14. Mccartgm, 22 April 2002, "Common Access Card, Test Lab-Concept of Operations", CTL ConOps v1.0.doc, p. 1.
15. Steed, C., Web-based Training, Gower Publishing Limited, Brookfield, Vermont, 1999.

BIBLIOGRAPHY

Adams, C. and Lloyd, S., *Understanding Public-Key Infrastructure-Concepts, Standards, and Deployment Considerations*, Macmillan Technical Publishing, Indianapolis, Indiana, 1999.

CAC Release 1.0 ICC Requirements v1.1 020801.pdf.

[www.dmdc.osd.mil/smartcard/images/CACRelease1ICCRequirementsv1.pdf] Accessed March 2004.

DISA, "Department of Defense Class 3 Public Key Infrastructure (PKI) End User Trainee Guide," July 2000, [<http://iase.disa.mil>] Accessed March 2004.

DISA's Introduction to Public Key Infrastructure and Applications:
[[https://infosec.navy.mil/PKI/Intro to pki.ppt](https://infosec.navy.mil/PKI/Intro%20to%20pki.ppt)] Accessed March 2004.

DoD PKI Resources and Documentation CD, 3rd ed., DoD PKI Program Management Office, May 2001.

Galik, D., "PKI and the Navy", CHIPS, January 2000,
[http://www.norfolk.navy.mil/chips/archives/00_jan/pki.htm] Accessed March 2004.

Green, R. M., "Public Key Infrastructure: The Enabler for DoD e-Bus," January 2001,
[rmgree2@missi.ncsc.mil] Accessed March 2004.

[http://64.4.26.250/cgi-bin/linkrd?_lang=EN&lah=e5e71c63ff0ebf83c1ceba9631f1dae5&lat=1051202136&hm__action=http%3a%2f%2fsearchsecurity%2etechtargget%2ecom%2fripsIndex%2f0%2c289482%2csid14_tax286152_alpD_idx0%2c00%2ehtml] Accessed March 2004.

[<http://disa.mil/infosec/pkieca>] Accessed March 2004.

[http://egov.gov/smartgov/information/cac_case_study.doc] Accessed March 2004.

[<http://falcon3.ncr.disa.mil>] Accessed March 2004.

[<http://iase.disa.mil/PKI/index.html>] (restricted to persons in the .mil and .gov domains)
Accessed March 2004.

[<http://iase.disa.mil/pki/index.html>] Accessed March 2004.

[<http://iase.disa.mil/PKI/PKICSPage.html>] (restricted to persons in the .mil and .gov domains)
Accessed March 2004.

[<http://jitec.fhu.disa.mil/pki/faq/whatis.html>] Accessed March 2004.

[http://www.artisoft.com/wp_pki_intro.htm] Accessed March 2004.

[<http://www.c3i.osd.mil/org/sio/ia/pki.html>] Accessed March 2004.

[<http://www.dmdc.osd.mil/smartcard>] Accessed March 2004.

[[https://infosec.navy.mil/PKI/Intro to pki.ppt](https://infosec.navy.mil/PKI/Intro%20to%20pki.ppt)] (DISA's Introduction to Public Key Infrastructure and Applications) Accessed March 2004.

[https://infosec.navy.mil/PKI/pki_101.ppt] (SPAWAR's PKI 101) Accessed March 2004.

[[https://infosec.navy.mil/PKI/what is pki.html](https://infosec.navy.mil/PKI/what_is_pki.html)] Accessed March 2004.

Introduction to Public Key Technology and the Federal PKI Infrastructure, D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang, NIST, 26 February 2001.

Marcia L. Ziemba, "A training framework for the department of defense public key infrastructure", Master's Thesis Naval Postgraduate School, Monterey, California, September 2001.

Morris, D., "Public Key Infrastructure (PKI) Overview," 2001, morrisde@hqmc.usmc.mil.

Mukul Pareek, "Digital Signatures, Digital Certificate And PKI", [<http://www.financeoutlook.com/modules.php?name=News&file=article&sid=12>], Accessed March 2004.

Navy PKI Primer: [https://infosec.navy.mil/PKI/PKI_primer_061801.pdf] Accessed March 2004.

PKI: Implementing and Managing E-Security, Andrew Nash, et al., McGraw-Hill, 2001.

"Public Key Infrastructure – PKI," [<http://www.id2tech.com/topmenu/smartcard/pki.asp>] Accessed March 2004.

United States Marine Corps, "Public Key Infrastructure (PKI) End Users Class – Trainee Guide," 2000, [<https://www.noc.usmc.mil/secure/PKI/default.htm>] Accessed March 2004.

What is PKI? [[https://infosec.navy.mil/PKI/what is pki.html](https://infosec.navy.mil/PKI/what_is_pki.html)] Accessed March 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. George Bieber
OSD
Washington, D.C.
4. RADM Joseph Burns
Fort George Meade, Maryland
5. Deborah Cooper
DC Associates, LLC
Roslyn, Virginia
6. CDR Daniel L. Currie
PMW 161
San Diego, California
7. LCDR James Downey
NAVSEA
Washington, D.C.
8. Richard Hale
DISA
Falls Church, Virginia
9. LCDR Scott D. Heller
SPAWAR
San Diego, California
10. Wiley Jones
OSD
Washington, D.C.
11. Russell Jones
N641
Arlington, Virginia

12. David Ladd
Microsoft Corporation
Redmond, Washington
13. Dr. Carl Landwehr
National Science Foundation
Arlington, Virginia
14. Steve LaFountain
NSA
Fort Meade, Maryland
15. Dr. Greg Larson
IDA
Alexandria, Virginia
16. Ray A. Letteer
Head, Information Assurance, HQMC C4 Directorate
Washington, D.C.
17. Penny Lehtola
NSA
Fort Meade, Maryland
18. Ernest Lucier
Federal Aviation Administration
Washington, D.C.
19. CAPT Sheila McCoy
Headquarters U.S. Navy
Arlington, Virginia
20. Dr. Ernest McDuffie
National Science Foundation
Arlington, Virginia
21. Dr. Vic Maconachy
NSA
Fort Meade, Maryland
22. Doug Maughan
Department of Homeland Security
Washington, D.C.

23. Dr. John Monastra
Aerospace Corporation
Chantilly, Virginia
24. John Mildner
SPAWAR
Charleston, South Carolina
25. Marshall Potter
Federal Aviation Administration
Washington, D.C.
26. Dr. Roger R. Schell
Aesec
Pacific Grove, California
27. Keith Schwalm
Good Harbor Consulting, LLC
Washington, D.C.
28. Dr. Ralph Wachter
ONR
Arlington, Virginia
29. David Wirth
N641
Arlington, Virginia
30. Daniel Wolf
NSA
Fort Meade, Maryland
31. CAPT Robert Zellmann
CNO Staff N614
Arlington, Virginia
32. Chairman, Code CS
Naval Postgraduate School
Monterey, California
33. Chairman, Code IS
Naval Postgraduate School
Monterey, California

34. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, California
35. J. D. Fulp
Naval Postgraduate School
Monterey, California
36. Glenn Cook
Naval Postgraduate School
Monterey, California
37. LCDR Vasileios D Athanasopoulos
Hellenic Navy
Athens, Greece