NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INSTALLATION, CONFIGURATION AND OPERATIONAL TESTING OF A PKI CERTIFICATE SERVER AND ITS SUPPORTING SERVICES

by

Vanessa P. Ambers
and
Amanda M. Kelly

June 2004

Thesis Advisor: J. D. Fulp
Second Reader: Dan C. Boger

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Installation, Configuration and Operational Testing of a PKI Certificate Server and Its Supporting Services			**5. FUNDING NUMBERS**
6. AUTHOR(S) Vanessa P. Ambers and Amanda M. Kelly			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Public key infrastructure (PKI) was created to provide the basic services of confidentiality, authenticity, integrity and non-repudiation for sensitive information that may traverse public (un-trusted) networks. This thesis provides a brief description of the background and functional components of a PKI, and then "builds" a PKI to be used for research at the Naval Postgraduate School (NPS). Deficiencies of this PKI with respect to DoD PKI policy are delineated. The thesis addresses details of software selection, installation, configuration and operation; using Netscape's Certificate Management System as its Certificate Authority application of choice. The functionality of this PKI was validated by testing all major certificate life-cycle events (creation, archival, revocation, validation, etc.) All but two of these tests were successful—key escrow and revocation checking—and thus these two remain to be addressed by further work to make the NPS PKI fully functional.

14. SUBJECT TERMS Public Key Infrastructure, PKI, Certificate Authority			**15. NUMBER OF PAGES** 182
			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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INSTALLATION, CONFIGURATION AND OPERATIONAL TESTING OF A PKI CERTIFICATE SERVER AND ITS SUPPORTING SERVICES

Vanessa P. Ambers
Lieutenant Commander, United States Navy
B.S., Morris Brown College, 1993

Amanda M. Kelly
First Lieutenant, United States Air Force
B.S., Colorado School of Mines, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2004

Authors: Vanessa P. Ambers

Amanda M. Kelly

Approved by: J. D. Fulp
Thesis Advisor

Dan C. Boger
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Public key infrastructure (PKI) was created to provide the basic services of confidentiality, authenticity, integrity and non-repudiation for sensitive information that may traverse public (un-trusted) networks. This thesis provides a brief description of the background and functional components of a PKI, and then "builds" a PKI to be used for research at the Naval Postgraduate School (NPS). Deficiencies of this PKI with respect to DoD PKI policy are delineated. The thesis addresses details of software selection, installation, configuration and operation; using Netscape's Certificate Management System as its Certificate Authority application of choice. The functionality of this PKI was validated by testing all major certificate life-cycle events (creation, archival, revocation, validation, etc.) All but two of these tests were successful—key escrow and revocation checking—and thus these two remain to be addressed by further work to make the NPS PKI fully functional.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....1
B. STATEMENT OF PROBLEM....1
1. Scope and Assumptions....2
C. RESEARCH OBJECTIVES....3
1. Primary Research Question....3
2. Subsidiary Research Questions....3
D. ORGANIZATION....4

II. WHAT IS PKI?....5
A. CRYPTOGRAPHY....5
B. PKI DEFINED....5
C. DIGITAL SIGNATURES....6
D. FUNCTIONAL COMPONENTS....9
1. End Entity....9
2. Certificate Authority....10
3. Repository....11
4. Registration Authority....11
E. CERTIFICATES....13
F. CERTIFICATE FORMAT....14
G. SUMMARY....15

III. NPS CISR LAB....17
A. DESCRIPTION....17
B. FACILITY DEFICIENCIES....17
C. ADJUSTMENTS FOR FULL COMPLIANCE....19
1. Physical Access....19
2. Procedural Controls....19
3. Personnel Controls....20
4. Computer Security Controls....21
5. Network Security Controls....21
D. SUMMARY....22

IV. SELECTION OF EQUIPMENT AND SOFTWARE....23
A. HARDWARE....23
B. SOFTWARE....23
1. Software Selection....23
2. CMS Components....24
3. CMS Subsystems....25
4. Nuts and Bolts....25
a. HTTP and JAVA Servlets....27
b. NSS....28
c. JSS and the JAVA/JNI Layer....28

d. PKCS #11 ..... *28*
e. Command Line Tools *29*
C. INSTALLATION ISSUES 29
D. FUNCTIONAL OVERVIEW 32
1. Interfaces 33
a. Administrative Interface *33*
b. Agent Interface *34*
c. Non-SSL and SSL Interface *35*
2. Users and Groups 36
3. Connecting the Subsystems 37
4. Certificates 40
a. Certificate Enrollment *41*
b. Certificate Renewal *42*
c. Owner Certificate Revocation *42*
d. Agent Revocation *43*
5. Jobs and Notifications 44
a. Notifications *44*
b. Jobs *45*
6. CRL and Publishing 46
7. Certificate Profiles 48
8. Key Archival and Recovery 50
a. Key Archival *51*
b. Key Recovery *51*

V. VALIDATION OF CERTIFICATE LIFE-CYCLE FUNCTIONALITY 55
A. LIFE-CYCLE TEST SETUP 55
B. CONDUCTING THE TESTS 56
1. Certificate Request, Request Approval and Import 56
2. Digital Signature and Encryption Testing 58
a. Manually Importing a CRL *59*
3. Certificate Expiration and Renewal 61
a. Renewal Notification *61*
b. Verification of Expiration *62*
c. Certificate Archival and Retrieval Following Expiration *63*
d. Certificate Renewal *63*
4. Certificate Revocation 64
a. Revocation by User *64*
b. Revocation for Cause *65*
c. Revocation Issues *65*
C. SUMMARY OF RESULTS 66
D. ADJUSTMENTS 67

VI. CONCLUSIONS 69
A. OBSERVATIONS 69
B. ISSUES 69
C. FOLLOW ON WORK 70

APPENDIX **73**
LIST OF REFERENCES **159**
INITIAL DISTRIBUTION LIST **161**

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Digital Signature Process 8
Figure 2. PKI Process Flow 12
Figure 3. Netscape CMS Server Group after Initial Installation 24
Figure 4. CMS Architecture 27
Figure 5. Certificate Manager, Registration Manager and Data Recovery Manager in Separate Instances. 30
Figure 6. One Server Group with Two CMS Instances. 31
Figure 7. Multiple Server Groups 32
Figure 8. A View from the Netscape Console that Controls the CA. 34
Figure 9. Screen Shot of the SSL End-Entity Interface of the RA. 36
Figure 10. Certificates Associated with a Specific User 37
Figure 11. Information Associated with a Subsystem Connector. 38
Figure 12. Manage Certificates Window 40
Figure 13. Certificate Renewal Page 42
Figure 14. SSL End-Entity page for Certificate Revocation. 43
Figure 15. Notification that Can Be Enabled in the CA. 45
Figure 16. Job Instance Editor for the Certificate Renewal Job 46
Figure 17. MasterCRL Configuration in CA's Console 47
Figure 18. Publishing Enabled on the CA 48
Figure 19. Certificate Profile Instance List and Plug-in Selection for a New Profile 49
Figure 20. Certificate Profile Policy Editor for Certificate Extension Addition 49
Figure 21. Creation of Certificate Profile Instance 50
Figure 22. How the Key Archival Process Works 51
Figure 23. DRM Recovery Agent Scheme 52
Figure 24. The Agent-initiated Key Recovery Process 53
Figure 25. SSL End-Entity Page of RA. 57
Figure 26. Certificate Request as Viewed from the RA's Agent Interface. 58
Figure 27. Message Security Properties without a Valid CRL. 59
Figure 28. CA End-Entity Page 60
Figure 29. Successful verification of certificate after a manual import of the CRL. 61
Figure 30. Certificate Renewal Notification Email 62
Figure 31. Verification of Certificate Expiration. 62
Figure 32. User Certificate Renewal End-Entity Page 63
Figure 33. User Certificate Revocation Form 65

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Description of Key Employment. 8
Table 2. Public Key Infrastructure (PKI) Functions 13
Table 3. Recommended Firewall Configurations 22
Table 4. Test Certificate Use and User 56
Table 5. Summary of Certificate Tests Results....67

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I dedicate this thesis in memory of my mother, Olivia Ambers, who lost her battle to colon cancer, during my time at NPS. Mom, I miss you and love you dearly. I know your watching over me as my personal angel. I thank my Lord and Savior, Christ Jesus for helping me to endure. – Vanessa Ambers

We would like to give special thanks to…

Mike Williams, Paul Clark, Gary Delgado, Victor Beach, Triet Vuong, Jason Hershcopf and Jacqueline Villasenor for their unbridled support, wisdom and knowledge in helping us obtain our thesis goals.

To our editors Cecily and Edward Kelly and Nancy Sharrock thanks for taking an extra glance to produce a magnificent product.

To our thesis advisor J.D. Fulp thanks for your guidance down the bumpy road to PKI.

To our sisters Mada, Maudrid, Katrena, Shonda, Teresa and Colby we thank you for your availing support and love.

To the many friends and family members to numerous to mention by name that provided words of encouragement, through your phone calls, emails and prayers were extremely grateful.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Gone are the days are in which human beings correspond via carrier pigeons, telegraphs, railroads, telephones and the Postal Service. In today's society, people are demanding immediate data exchange most likely provided by the Internet. Since its invention in the late 1950's, the Internet has become a global focal point on which people rely for personal, business, and even military use. In each arena, from personal to military use, it is vital that the data exchange be conducted in a secure environment. Thus, the introduction of Public Key Infrastructure (PKI), which is a promising new technology to support the secure exchange of data over the Internet. PKI can support a wide variety of Internet applications including electronic mail, virtual private networks, secure web access and custom applications. It allows a sender to "sign" data digitally, and for the recipient to verify the originator of the data and to ensure the data has not been modified without the recipient's knowledge. PKI provides the user with four basic security services: confidentiality, integrity, authenticity and non-repudiation.

In today's society, these information security services are vital to the performance of any organization and are essential services required by the Department of Defense (DoD) as it engages heavily in sensitive communications. The DoD has taken an aggressive approach in establishing a PKI that promises to support its diverse set of missions and operations. "The implementation of PKI in the DoD will enhance military operations in the tactical, joint, and combined operational environments, as well as improved interoperability with allies, coalition forces, civil agencies, and business partners."[1] This will ensure operational effectiveness when U.S. forces participate in ongoing campaigns to promote democracy, defend American sovereignty, liberate countries and combat terrorism.

B. STATEMENT OF PROBLEM

A Public Key Infrastructure (PKI) is a core enabler for more secure communications in a computer network environment. It is defined as an infrastructure for

[1] DoD Public Key Infrastructure Program Management Office, "PKI Roadmap for the DoD, Version 5.0," December 18, 2000.

establishing a secure method for exchanging digital information. It is a combination of cryptographic methods and software that integrates the use of digital signatures, digital certificates and certificate authorities into a network security architecture capable of managing the process. Properly implemented and managed, a PKI can provide the necessary mechanism whereby all the information assurance attributes of confidentiality, integrity, authenticity and non-repudiation can be achieved. The success of any PKI is primarily determined by the answers to three questions: 1) How trustworthy is the binding of the declared identity in a certificate with that of its associated public key? 2) How well are private keys kept safe from misuse? 3) Is the strength of the certificate validation checking mechanism sufficient?

In 1997, the Deputy Defense Secretary, Dr. John Hamre, exhorted that the DoD would provide a solid foundation for information assurance capabilities across all its Departments consistent with its operational imperatives and missions. He announced a new DoD policy encouraging the widespread use of PKI to facilitate a paperless organization and to provide secure communications. Later, DoD mandated that all its infrastructures be prepared to issue and use Class 3 certificates by October 2002. Currently, the DoD Chief Information Officer (CIO) has amended this requirement to read all sites will, "continue to work towards achieving these important milestones, as soon as possible."[2] This amendment was due to a DoD-wide failure to implement the myriad of infrastructure components required to achieve this overly optimistic milestone.

The DoD is seeking help from within its own organizations, the commercial sector, and research organizations, such as the Naval Postgraduate School, to assist in achieving its goal of Department-wide PKI usage.

1. Scope and Assumptions

The purpose of this proposed thesis work is to create a test PKI for research use at the Naval Postgraduate School. The goal will be to implement the PKI using commercially available products and services so that it is as close to DoD compliance as possible given the constraints of the NPS physical facilities and research money available. The PKI prototype will integrate DoD compliant devices, services and

[2] DoD Chief Information Officer Memorandum, "DoD PKI Milestones Update," October 7, 2003.

technologies into a fully functional CA. A PKI test facility available on-site at NPS will enable ensuing faculty and thesis students to conduct further research into the DoD's most provocative questions to make their goal of Department-wide PKI usage a reality.

C. RESEARCH OBJECTIVES

1. Primary Research Question

- How to implement a Certificate Server and its supporting certificate issuance, archival, revocation and validation infrastructure?

2. Subsidiary Research Questions

- What are all the functional components of a CA?
- What are DoD's specified administrative and policy requirements concerning operating a CA?
- What are the infrastructure facility deficiencies of the NPS CISR CA labs that may preclude it from being in full compliance with a DoD-compliant CA?
- What are the technical requirements regarding the operation of a CA server and its supporting issuance, archival, revocation, and validation infrastructure?
- What hardware is necessary to implement a fully functional CA?
- What software is necessary to implement a fully functional CA?
- What is the proper communicative interaction between the Local Registration Authority (LRA) server, the Registration Authority (RA) server, the Certificate Authority (CA) server, the certificate archival directory, and the revocation and validation servers/services?
- What are the proper means for registering PKI certificate owners?
- What are the proper means for making certificates available to the user community?
- What is the proper means for maintaining archives of inactive certificates and keys?
- What is the proper means for maintaining a private key recovering agent (KRA)?
- What is the proper means for supporting certificate revocations that may occur for reasons other than normal certificate expiration?
- What are the proper means for providing a mechanism for users of the CA's certificate to assess the current validity status of those certificates?

- What should be included in a CA Users' Manual that would facilitate on-going operations of the test CA?

D. ORGANIZATION

This thesis is composed of six chapters and an appendix.

Chapter I: Introduction – This chapter introduces the topic of Public Key Infrastructure (PKI) and discusses the benefits of having a PKI available for testing at the Naval Postgraduate School.

Chapter II: What is PKI? – This chapter provides an overview of PKI to include its components and related products and services.

Chapter III: Naval Postgraduate School's Center for Information Systems Security Studies and Research (CISR) Lab – This chapter provides a broad overview of the NPS CISR lab, to include deficiencies of the lab in meeting DoD CA requirements and what adjustment would need to occur for the lab to be in compliance with those requirements.

Chapter IV: Selection of Equipment and Software - This chapter outlines the choice of hardware and software utilized to implement the test PKI and an inter-component functional overview of the software.

Chapter V: Validation of Certificate Life-Cycle Functionality – This chapter describes the results from the certificate life-cycle tests performed to validate the PKI performance.

Chapter VI: Conclusion – This chapter summarizes the main ideas presented in the previous chapters, stating observations and issues experienced in the completion of the thesis, and suggesting potential areas for continued research on this topic.

Appendix: User's Guide - This guide has two parts. The first is a basic installation guide of the software and hardware utilized to construct the test PKI facility. The second provides the user with instructions and diagrams for all tasks required for certificate management.

II. WHAT IS PKI?

A. CRYPTOGRAPHY

Public Key Infrastructure has its early roots in cryptography, which can be traced to Julius Caesar's reign over Rome. The Webster dictionary defines cryptography as the enciphering or deciphering of messages in secret code or cipher. To encipher data is to take plaintext to an unreadable text and decipher it to reverse the process back to comprehensible text. Data is often enciphered to prevent eavesdropping so that an unlikely recipient cannot interpret the captured information. The two basic forms of cryptography are symmetric and asymmetric. A symmetric cryptographic algorithm applies the same key for encryption and decryption. Whereas Diffie and Hellman introduced asymmetric cryptography in the late 1970's[3], which became the basis for PKI. Asymmetric cryptography utilizes two mathematically related keys to encipher and decipher data.

B. PKI DEFINED

The DoD defines PKI as, "the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communication and business transactions on networks."[4] Most importantly, PKI permits users with no preexisting relationship to communicate securely regardless of the distance between them through a commonly shared certificate "chain of trust". PKI allows an organization to enjoy the basic services of confidentiality, data integrity, identity and authenticity and non-repudiation. The National Institute of Standards and Technology (NIST) define these services as:[5]

> Confidentiality services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.

---

[3] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Transformation Theory 22, pp. 644-654, 1976.

[4] Defense Information Systems Agency, "DoD Public Key Infrastructure Introduction," [http://jitc.fhu.disa.mil/pki/intro.html], January 12, 2004. Accessed June 2004.

[5] National Institute of Standards and Technology, "Introduction to Public Key Technology and the Federal PKI Infrastructure," February 26, 2001.

> Data Integrity services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.
>
> Identification and authentication services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.
>
> Non-repudiation services prevent an individual from denying that previous actions had been performed. The goal is to ensure that all the recipients of the data is assured of the sender's identity.

These services, combined with an organization's desire to enhance the security of their data and to minimize the amount of paper generated by their organization, has given momentum to the use of PKI, which is essential to an organization's growth. Any enterprise intending to maximally leverage use of the Internet should strongly consider utilizing PKI. Due to the various commercial products and configurations available, a committee was formed to generate a standard for implementing PKI and its related products and services. The PKIX (PKI X.509) working group was formed in September 1995 to establish and develop Internet standards to support an X.509-based PKI. Today, the X.509 standard is widely accepted and PKIX has produced several informational and standard track documents in support of PKI.[6] This thesis will make frequent reference to the X.509 guidelines and achievements.

C. DIGITAL SIGNATURES

The DoD policy states that users who have the capability to sign emails digitally must always do so after 1 October 2002.[7] The user can configure a workstation to sign and encrypt documents automatically. The enciphering of data ensures the confidentiality of the information sent over the worldwide web. Digital signatures provide for the remaining services of data integrity, authentication and non-repudiation. Public key cryptography involves the public distribution of an encryption key string, or public key, to the intended recipients of data. The sender will maintain his private key in a secure location.

---

[6] Internet Engineering Task Force, "Public-Key Infrastructure (X.509) (pkix)," [http://www.ietf.org/html.charters/pkix-charter.html], May 18, 2004. Accessed June 2004.

[7] Arthur Money, "DoD PKI Policy Memorandum," August 12, 2000.

A digital signature generation process is begun by sending the original data through a "one way hash algorithm." A hash algorithm produces an unreadable, condensed version of the original message, called a message digest, by using one of the listed hash algorithms:[8]

- **MD5** is a 128-bit message digest function developed by Ron Rivest.
- **SHA-1** is a hashing algorithm similar in structure to MD5, but produces a digest of 160 bits (20 bytes). Due to the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reason, SHA-1 is preferred to MD5.
- **HMAC** is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus, it is possible to refer to HMAC-MD5 and HMAC-SHA1.

The message digest is then encrypted using the sender's private key, thus creating the digital signature. The message and the digital signature are then sent to the recipient. The recipient must then verify the digital signature. She starts this by hashing the received message using the same hash algorithm the sender did. The recipient uses the sender's public key from the sender's certificate to decrypt the digital signature (the encrypted message digest) that was sent with the message. If the message digests are identical than the digital signature has been verified. The verified digital signature assures the recipient that the message was sent from the rightful sender, data authenticity, and that data has not been altered, data integrity. These steps are completed by the CMS, and are therefore transparent to the users. The process of digital signing and verification appears in Figure 1.

[8] Cryptography World, "The Cryptography Guide," [http://www.cryptographyworld.com/algo.htm], 2003. Accessed June 2004.

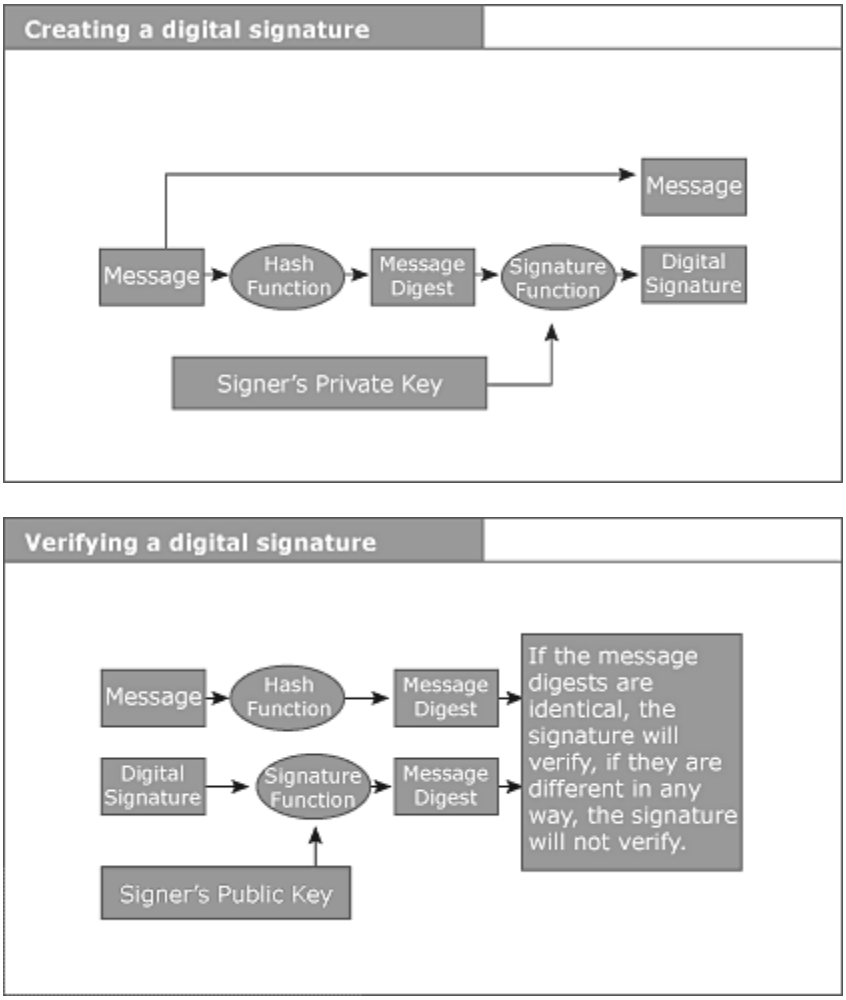


Figure 1. Digital Signature Process[9]

This process can be very confusing as to what key to use when and for what reason and by whom. Therefore, Table 1 summarizes which key to use.

Key Function	**Key Used**	**Key Owner**
Encrypt data	Public key	Receiver
Sign data	Private key	Sender
Decrypt data	Private key	Receiver
Verify Signature	Public key	Sender

Table 1. Description of Key Employment.

[9] Digital Signature Trust, "PKI Basics Digital Signatures and Public Key Infrastructure (PKI) 101," [http://wwwdigitalsignaturetrust.com/support/pki_basics.html]. Accessed June 2004.

D. FUNCTIONAL COMPONENTS

The next section focuses on the components of the PKI architecture. PKI provides, "the framework and services that provide for the generation, production, distribution, control and accounting of public key certificates."[10] It unites hardware and software components, policies and procedures in such a way as to be able to zealously communicate with greatly reduced fear of compromise. It provides the user with the basic services of confidentiality, data integrity, non-repudiation and authenticity.

Different organizations choose to configure their PKI utilizing the various available commercial products. The PKI should be tailored to the organizational needs of an enterprise. Although the configuration may vary, the basic components remain the same. The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) working group has identified several formal and generic models of a certificate-based architecture utilizing the basic components: of end entity (i.e., certificate owner, and user), certificate authority, certificate repository and registration authority

1. End Entity

This term is often used to denote the personnel aspect of PKI. However, it also includes devices such as routers, servers or other entities that require certificates to enable certificate based authentication or encryption. Depending on the organizational standard, it may be referred to as the end user, relying party, or subscriber. Regardless of the terminology used, the end entity is the person or device name identified in the subject field of the certificate. Once enrolled, the end entity is bound to the public key contained in the certificate and identified by the distinguished name contained in the certificate. A relying party is included as a component in some PKI infrastructures as an end entity. The X.509 states:

> A relying party is the entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the binding the Subscriber's name to a public key. A relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

[10] Space and Naval Warfare Systems Command Information Systems Security Information Warfare Defense Program Management Office, "Department of Defense Public Key Infrastructure Primer, Version 3.0," 18 June 2001.

2. Certificate Authority

There are three types of CA: self signed, subordinate and root CAs. They are defined as:[11]

- Self-signed CA. In a self-signed CA, the public key in the certificate and the key used to verify the certificate are the same. Some self-signed CAs are root CAs.

- Subordinate CA. In a subordinate CA, the public key in the certificate and the key used to verify the certificates are different. The process where one CA issues a certificate to another CA is known as cross-certification.

- Root CA. A root CA is a special class of CA, which is trusted by a client and is at the top of a certification hierarchy. All certificate chains terminate at a root CA. The root authority must sign its own certificates because there is no higher certifying authority in the certificate hierarchy.

As a result of the policies associated with the various CAs, organizations publish Certification Practice Statements (CPS) to determine policy standards for operating CAs. A CA could be responsible for issuing certificates in accordance with one or more certificate policies associated with the aforementioned CA types. The X.509 states, "A CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issues." The CA is the core element of the PKI, and it creates, signs, stores and issues certificates to end entities. A CA accepts a certificate request, and after verification, will use its private key to assign a digital signature to the certificate. The signature process effectively binds the end entity's (i.e., the certificate owner's) identity with his/her public key that is stored within the certificate. Once signed, the certificate is issued to the end entity.

[11] Microsoft, "Microsoft Windows 2000 Server, Cryptography and PKI Basics," 2000.

3. Repository

A repository is a generic term used to denote any method for storing certificates and CRL's so that they can be retrieved by the end entity[12]. A certificate authority can be configured to generate a certification revocation list (CRL). A CRL is a compilation of certificates revoked prior to their normal expiration date. Certificates are revoked due to a number of reasons, such as; key compromise, CA compromise, termination of employment, or change of identifying information in the certificate. The certificates are listed in the CRL by serial number and are time stamped. CRL's can either be online, in which case the revocation list is pulled by the user, or offline, in which case the CA pushes the revocation list to one of its directories. The online version utilizes the Online Certificate Status Protocol (OSCP), which checks the status of certificates without tasking the CA. The off-line version encompasses the subscriber using the Lightweight Directory Access Protocol (LDAP), the Hyper Text Transfer Protocol (HTTP), or the File Transfer Protocol (FTP) to view the status of certificates prior to authenticating a certificate. Each of these standards reduces the overhead of the CA by off-loading more of the CRL functionality.

4. Registration Authority

The RA is an optional component that can assume a number of administrative functions from the CA.[13] Through a trusted relationship with the CA, the RA can initiate, renew and/or revoke a certificate request. The RA acts as the middleman between the CA and trusted agents to process requests for enrollment, renewal and revocation, and to sending the signed request to the certificate manager (CM). It will then distribute the approved request from the CM to the requesting agent. The RA cannot issue, renew, or revoke certificates, nor can it or publish CRL's as those functions are specific to the CA.

The RA can be used for added protection for the CM by placing it outside the firewall. The RA will determine if the request is from a trusted agent prior to sending the request to the CM that should be located behind the firewall.

Figure 2, illustrates the high level activities associated with the PKI without the optional RA displayed.

---

[12] PKI Forum, "PKI Basics – A Technical Perspective," November 2002.

[13] Ibid.

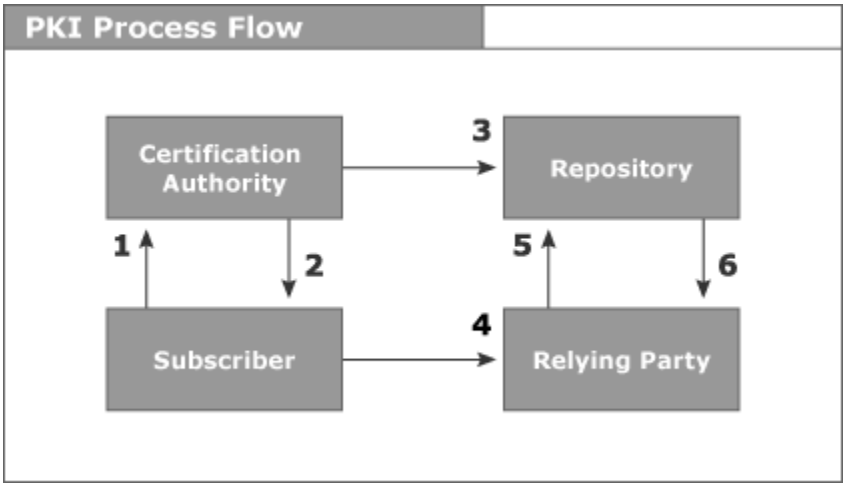


Figure 2. PKI Process Flow[14]

Step 1. Subscriber applies to Certification Authority for Digital Certificate.

Step 2. CA verifies identity of Subscriber and issues Digital Certificate.

Step 3. CA publishes Certificate to Repository.

Step 4. Subscriber digitally signs electronic message with a Private Key to ensure Sender Authenticity, Message Integrity and Non-Repudiation and sends to Relying Party.

Step 5. Relying Party receives message, verifies Digital Signature with Subscriber's Public Key, and goes to Repository to check status and validity of a Subscriber's Certificate.

Step 6. Repository returns results of status check on Subscriber's Certificate to Relying Party.

Now, with a basic understanding of the components in the PKI provided. Table 2 depicts some common tasks associated with a PKI and the component that is responsible for implementing each task.

[14] Digital Signature Trust, "PKI Basics Digital Signatures and Public Key Infrastructure (PKI) 101," [http://www.digitalsignaturetrust.com/support/pki_basics.html]. Accessed June 2004.

Function	Description	Implementation
Registering users	Collect user information, verify identity	Function of CA, or separate RA
Issuing certificates	Create certificates in response to user or administrator request	Function of the CA
Revoking certificates	Create and publish Certificate Revocation Lists (CRLs)	Administrative software associated with the CA
Storing and retrieving	Make certificates and CRLs available to authorized users	Repository for certificates and CRLs in secure replicated directory service accessible via LDAP
Certificates and CRLs	Impose policy-based constraints on certificate chain, and validate if all constraints are met	Function of the CA
Policy-based certificate path validation	Time-stamp each certificate	Function of the CA or a dedicated Time Server (TS)
Key lifecycle management	Update, archive and restore keys	Automated in software or performed manually

Table 2. Public Key Infrastructure (PKI) Functions[15]

E. CERTIFICATES

> A public key certificate is a digitally signed statement that binds the value of a public key to the identity of the subject (person, device, or service) that holds the corresponding private key. By signing the certificate, the CA attest that the private key associated with the public key in the certificate is in the possession of the subject named in the certificate.[16]

A certificate provides a legally, binding exchange that cannot refute a person's identity. The recipient of the data is assured of a person's identity by the CA signing of the certificate. Certificates are issued across CAs and are assigned by classes with different assurance levels to establish a hierarchy. A "chain of trust" is initiated when a CA validates a user. Trust relationships are established among CAs, by issuing cross certifications forming trusted paths. When a user tries to validate a certificate from a user outside of his chain, the trusted relationships are used to validate that certificate. CAs

[15] Ray Hunt, "PKI and Digital Certification Infrastructure," [http://www.au-kbc.org/bpmain1/PKI/PKIieee.pdf], 2002. Accessed June 2004.

[16] Microsoft, "Microsoft Windows 2000 Server, Cryptography and PKI Basics," 2000.

can have numerous trust relationships established, each one having a different level of assurance associated with it. The assurance levels are provided as follows: Class 2 certificates are intended for low value unclassified information in a moderately protected environment. Class 3 certificates consist of class 2 assurances in addition to high value and discretionary access control information in highly protected environments. Class 4 handles unclassified high value mission critical information in minimally protected environments. Class 5 is reserved for high value, high-risk environment information. The X.509 requires a person's identity to be established by a database, supervisor or subscriber for class 2-assurance level. It requires a trusted agent to physically view a valid ID for class 3 and 4 assurances. The National Security Agency (NSA) determines class 5 assurance level requirements.

This thesis involved the use of Netscape software to build the prototype PKI. Netscape application recognizes the following certificate types:[17]

- Personal (or client) certificates: These certify the identity and public key of a client.
- Server (or site) certificates: These certify the identity and public key of a server.
- Secure email certificates: These certify the identity and public key of an email application user. It is also used to encrypt and decrypt email messages.
- CA certificates: These certify the identity and signing key of a certificate authority.

F. CERTIFICATE FORMAT

Currently, several certificate formats are available, but the most widely adopted meet the X.509 specification lauded by the International Telecommunication Union (ITU-T) and developed in 1988. "The X.509 certificate format has evolved through three versions – the 1988 version (v1), the 1993 version (v2), and a new version (v3) allows for

[17] Netscape Communications Corporation, "Understanding Certificates," [http://developer.netscape.com/docs/manuals/certificate/certagnt/overview.htm], 1997. Accessed June 2004

many certificate extension fields required for PKI, and it is recommended that PKI planning assume use of v3."[18] Regardless of the certificate version chosen, most have similar content. Every X.509 certificate consists of:[19]

- A data section which includes the following information:
  - The version number of the X.509 standard supported by the certificate.
  - The certificate's serial number. Every certificate issued by a CA has a unique serial number.
- An information section which includes the following information:
  - Information about the user's public key, including the algorithm used and a representation of the key itself.
  - The DN of the CA that issued the certificate.
  - The period during which the certificate is valid.
  - The DN of the certificate subject also called the subject name.
  - Optional certificate extensions, which may provide additional data used by the client or server.
- A signature section which includes the following information:
  - The cryptographic algorithm, or cipher, used by the issuing CA to create its own digital signature.
  - The CA's digital signature, obtained by hashing all the data in the certificate together and encrypting it with the CA's private key.

G. SUMMARY

In this chapter we reviewed the core of public key cryptography, which consists of using two mathematically related keys to encode and decode messages. The key pair includes one public key that is widely distributed and a private key. PKI provides the user

[18] Warwick Ford, "A Public Key Infrastructure for U.S. Government Unclassified but Sensitive Applications," September 1, 1995.

[19] Netscape Communications Corporation, "Administrator's Guide, Netscape Security Management System Version 6.1," [http://enterprise.netscape.com/docs/cms/61/cert/pdf/cms61admin.pdf], February 2003. Accessed June 2004.

with the basic services of confidentiality, integrity, authenticity and non-repudiation. It allows for secure communication between subscribers through the concepts of digital signatures and certificates. A PKI can be established in various arrangements, but the baseline PKI components of: certificate authority, end entity and repositories remain unchanged. An organization may decide to include the optional RA component to enhance the scalability of the CA. The next chapter will outline specific policy issues and how the CISR lab compares to DoD specifications for PKI implementation.

III. NPS CISR LAB

A. DESCRIPTION

Information security is a relevant aspect of DoD operations, and therefore, the use of PKI is becoming a more widely used practice. The Naval Postgraduate School's Center for Information Systems Security Studies and Research's (CISR) mission is to address the Information Assurance (IA) needs of the war fighter. NPS, through the CISR facility, has a highly motivated academic research group focused on issues of computer security, which makes it well suited to conduct research on PKI.

A test PKI system will enhance a student's understanding of the PKI allowing for additional research and special projects on the PKI registration process, key escrow and recovery, lifecycle of digital certificates and innovative ideas to improve PKI service implementation. In addition, a PKI in the CISR lab will provide a method for NPS to produce digital certificates during its participation in cyber attack/defend exercises conducted with other commands/services/schools/agencies (C/S/S/A). Portions of the lab equipment are connected to the internal NPS domain, with access to the outside world to allow for research and standard connectivity capability. Other portions are restricted to a private network to facilitate the isolation of cyber war games.

B. FACILITY DEFICIENCIES

The test bed PKI is located in the CISR lab on the fifth deck of Spanagel Hall room 500. The CISR lab is in use by a multitude of students, professors and research associates, and is viewed by escorted visitors several times per quarter. The facility has a cipher lock at each of three entrances with differing combinations. One combination allows individual access to Spanagel Hall's 500 and 511 CISR lab facilities.

The DoD Certificate Policy (CP) states, "CA equipment shall always be protected from unauthorized access."[20] The multi functional aspects of the CISR lab prevent NPS from meeting this requirement. Students from several classes each quarter have access to the lab at any given time during the day. Students working on their theses and students participating in special projects or exercises also have continuous access to the lab.

[20] Department of Defense Public Key Infrastructure Program Management Office, "X.509 Certificate Policy for the United States Department of Defense," December 11, 2003, Version 8.

Although an unspoken rule exists that no one will touch another's equipment or projects without consent, the CISR lab fails to meet the DoD CP requirements for physical access control.

Policy also dictates that if the lab is physically unattended for more than 24 hours, an intrusion detection system for physical access or security check should be incorporated. The security check is intended to ensure that the CA has not been tampered with and is in the proper mode of operation, and that security containers containing PKI related materials are properly secured, and physical security systems are operational. The security check would provide an extra layer of protection against unauthorized access. Guidance further states that a person or groups of people should be responsible for conducting the security checks. The adoption of the latter mandates the maintenance of a security schedule dictating the responsible individual with the date and time of this inspection.

For fire prevention and protection, the X.509 rescinded the need for a sprinkler system and fire extinguishers to be present in the area housing the CA. The CISR lab does not a have a sprinkler system but it does have a fire extinguisher located in the adjoining lab, as well as manual fire alarms and a halon system. The X.509 states that a descriptive approach for Certificate Management Authority (CMA) recovery from a disastrous fire should be included in an organization's Disaster Recovery Plan. Since the CISR lab is a research facility, it does not have a bona fide Disaster Recovery Plan. In the event of a disaster, the system will be "recovered" as best as possible by the system administrator.

Also, part of the Disaster Recovery Plan and a required mechanism for physical security, is the need for a redundant CA power source to allow for completion of any pending actions prior to a complete loss of power. The CISR facility does not have an uninterruptible power supply (UPS) associated with the PKI prototype. The Disaster Recovery Plan also includes the need for an offsite backup facility with periodic backups conducted on a weekly basis for continuously operated Class 3 CAs.[21] The PKI will provide functionality during cyber defense exercises and facilitate follow on research in

[21] Ibid.

PKI issues. It will not be used outside of NPS for real-world operations. Because the CMS is reserved for research purposes only and poses no threat to the CISR organization's network security or daily operations, the requirement to invest in a backup facility to protect the CMS data is not deemed essential. This thesis contains an installation guide that enables the PKI to be recreated in the event of total loss.

C. ADJUSTMENTS FOR FULL COMPLIANCE

1. Physical Access

Physical Security Adjustments that need to occur in the NPS CISR facility to make the PKI system DoD compliant would require additional funding, space and/or policy changes. All equipment designated for the PKI is required to be in a controlled environment. The CISR lab would have to designate a space for the CA in its current lab and restrict unauthorized access or acquire a new facility to house the CA. If a new facility is desired, DITSCAP, (DoD Information Technology Security Certification Accreditation Process), the certifying agent for all DoD IS, would have to approve the facility for accreditation to support a CA.[22] The facility would need its own air conditioning, power source, fire protection system and carbon dioxide detectors. Equipment would have to be protected from flooding by utilizing raised floors. An intrusion detection system would need to be employed due to the absence of personnel for periods greater than 24 hours. An off-site backup facility would have to be selected to store data in the case of a disaster wherein data is destroyed.

2. Procedural Controls

The DoD prepared a Certification Practice Statement (CPS) that, "Establishes the procedures which satisfy the Certificate Policy for the management of certificates within a Certificate Authority domain and states the operating procedures for the Certification Authority, clarifying the legal rights and obligations."[23] Because certificates are legally binding and can be upheld in a court of law, certain procedures must be instituted to ensure the integrity of the CA. The CPS has adopted specific policies to protect the DoD PKI architecture. The CPS states,

---

[22] United States Department of Defense, "Defense Information Infrastructure Certification Authority Certification Practices Statement for Release 3, Version 4.1, May 15, 2002.

[23] Space and Naval Warfare Systems Command Information Systems Security Information Warfare Defense Program Management Office, "Department of Defense Public Key Infrastructure Primer, Version 3.0," June 18, 2001.

> The trusted roles must be filled by a least two different individuals at a CA. Since all of these roles require UNIX "root" privileges, procedural two-person control will be used to access the CA system.[24]

This thesis was originally envisioned to adhere to the DoD standard for PKI implementation. The DoD defines two-person control as "the continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements."[25] In the CISR lab, an entire class may have complete access to the PKI, allowing them to make changes without visibility to other trusted agents. This security flaw will not be addressed since the CISR PKI will be used to create test certificates and will not be used in an official high assurance capacity.

The CPS further recommends the separation and appointment of individuals for the role of Certification Authority, Registration Authority, Local Registration Authority, Server Administrator, Code Signing Attribute Authority, System Administrator, ISSO, Crypto-Officer and Operator. The CPS guidance reads,

> The system administrator and crypto officer roles should never be combined. The ISSO role must be assigned to some one who does not have the operator role or the crypto officer role.

The CPS provides guidelines that may be tailored to an organization's needs. Therefore, the NPS CA does not have a delineation of such roles due to the use of the CA for research purposes, and whereby, one or more thesis students could perform any or all roles.

3. Personnel Controls

The X.509 dictates,

> Persons shall be selected for any CMA or other trusted role on the basis of loyalty to the United States, their trustworthiness, and integrity. CMAs may be US uniformed service members, or government civilian employees (Federal, State, or local) of any organization authorized by the PMA to possess and issue DoD PKI certificates in accordance with Section 1.3.3.1

[24] United States Department of Defense, "Defense Information Infrastructure Certification Authority Certificate Practices Statement for Class 3 Assurance Version 3.91," August 8, 2001.

[25] Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," [http://www.dtic.mil/doctrine/jel/doddict/data/t/05537.html], March 2004. Accessed June 2004.

> of this CP, or such organizations' contractors. All CMAs shall be US citizens. All persons filling trusted roles other than CMAs should be US citizens or hold a US security clearance.

It further states that background checks should be conducted on personnel placed in other trusted roles for the PKI. The CISR lab participants are comprised of U.S. citizens and students from approximately 30 other countries. The occasion might arise where the need to have a foreign national act in a privilege role may occur. Since the NPS CA is restricted to NIPRNET access and only generates "test" certificates (i.e., certificates whose signing CA are not recognized outside of the NPS lab domain) the requirements for U.S. citizenship, a security clearance and background check were not followed.

4. Computer Security Controls

"CA and OCSP Responder equipment used for CLASS 3 assurance infrastructures shall use operating systems that:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability."[26]

The workstation that houses the CA does not have an authenticated login currently installed. However, this can easily be implemented but is not viewed as a necessity since the CA is being utilized for research purposes. The CPS dictates that the workstation for the CA server passes a DITSCAP accreditation process. The NPS CA will not request DITSCAP certification due to its primary usage being research.

5. Network Security Controls

The DoD CPS requires the CA to be connected to a single network with the servers protected by a firewall and equipped with a mechanism to prohibit unauthorized physical access. Table 3 illustrates the DOD proposed configuration of firewalls. The NPS CISR lab is in compliance with the network security criteria with the exception of the physical access restrictive measure. Following the Solaris security precautions that daemons should not run as root, the default ldap port numbers were not used. Instead, ports 38900, 1027, 1037, and 1035 were used, which are also opened through the firewall.

[26] X.509.

(PRIVATE) Service	Port	Protocol	In	Out
HTTP	80	TCP	Y	Y
HTTPS	443	TCP	Y	Y
LDAP	389	TCP	Y	Y
LDAP	390	TCP	Y	Y
LDAPS	636	TCP	Y	Y
LDAPS	637	TCP	Y	Y
DNS	53	UDP	N	Y
SMTP	25	TCP	N	Y

Table 3. Recommended Firewall Configurations

D. SUMMARY

The DoD CPS and the X.509 standards were utilized and provided a roadmap for thesis students to follow in creating the PKI prototype. Due to the CISR lab PKI facility deficiencies and the desire to create a PKI for research purposes, the DoD recommendations were altered to meet the much less stringent security requirements of the NPS research environment. The following chapter will expound on the selection of equipment and software used to create the PKI.

IV. SELECTION OF EQUIPMENT AND SOFTWARE

A. HARDWARE

The CISR lab boasts a multitude of equipment and hardware components that are utilized by students, faculty and staff for research purposes, and lab exercises in support of class work. The equipment is also used to compete against other research institutions in cyber defense exercises. NPS, having just participated in a cyber defense competition in which two Sun Blade 100's were utilized, did not have follow-on work making them available for utilization. The DoD Root CA and the subsidiary CAs currently run on Sun boxes so the Sun Blades were optimal for a PKI installation in the CISR lab.

Installation and configuration of the PKI subsystems revealed that the Sun boxes did not have adequate memory. With each running only 256 MB of SDRAM, the machines responded poorly during configuration changes. A memory upgrade was required to support this research. Two 512 MB, 168-pin DIMM SDRAM PC133 memory chips were added to each box increasing the RMA to greater than 1 gigabyte. This memory increase helped with the processing speed of the CMS system during configuration changes and while all of the services installed were running simultaneously. The improved performance proved sufficient to support this project.

B. SOFTWARE

1. Software Selection

The initial research into the current DoD implementation and the desire to implement a DoD compliant PKI, led to the selection of the Netscape Certificate Management System (CMS). DISA, Defense Information Systems Agency, entered a license agreement for all of DoD with the AOL-Sun-Netscape alliance to offer their PKI software for various implementations throughout DoD. When the license agreement ended, DISA renewed the license with America Online Strategic Business Solution (AOL SBS). Netscape has created multiple version of its CMS, allowing it to run on many different platforms. Netscape CMS was chosen for this project because

- It is the current DoD standard
- Licenses were available under the DISA enterprise license, and
- There was a version compatible with the Sun systems at NPS.

2. CMS Components

The Netscape CMS architecture works with a GUI interface, the Netscape Console, and three different systems, the Administration Server, the Directory Server, and the CMS itself. Each server is referred to as an instance in the Netscape Console and one instance of each of the three systems is installed in a server group during the initial software installation (Figure 3).

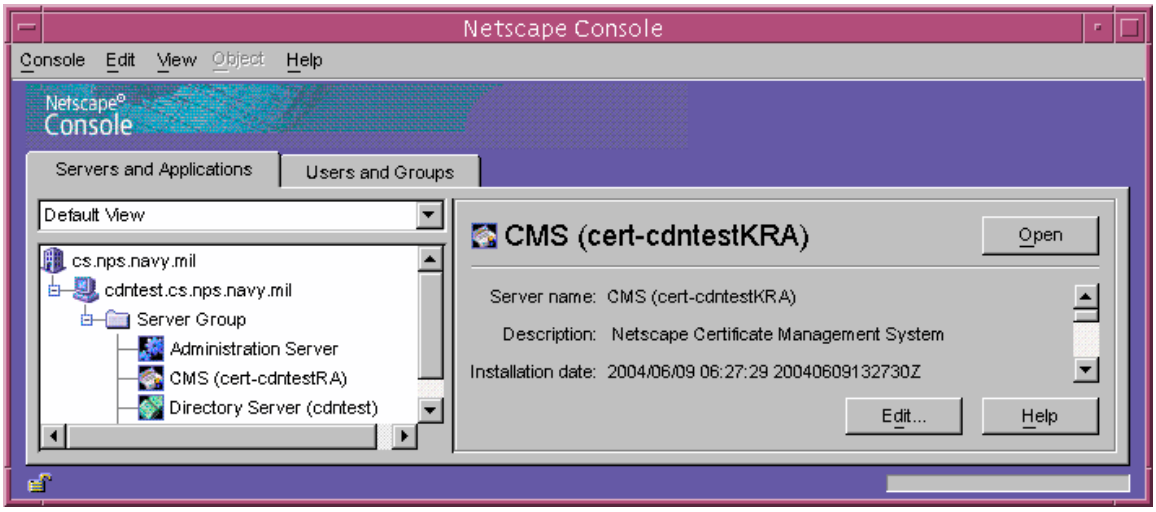


Figure 3. Netscape CMS Server Group after Initial Installation

- Netscape Console "is the front-end management application for Netscape software in your enterprise. It finds all servers and applications registered in your configuration directory, displays them in a graphical interface, and lets you manage and configure them. In addition, Netscape Console provides graphical tools for locating and managing entries in the user directory."[27]
- Administration Server – controls the resources used by the directory server instance and the CMS instance. It executes programs "to modify the server and application settings that are stored in the configuration directory or to change the port number that a server listens to."[28]

---

[27] Netscape Communications Corporation, "Managing Servers with Netscape Console," [http://enterprise.netscape.com/docs/cms/61/admin/ag/1_intro.htm#11284], August 2002. Accessed June 2004.

[28] Ibid.

- Directory Server "is a robust, scalable server designed to manage an enterprise-wide directory of users and resources. It is based on an open-systems server protocol called the Lightweight Directory Access Protocol (LDAP)."[29]
- CMS – hosts "a highly configurable set of software components and tools for creating, deploying, and managing certificates."[30]

3. CMS Subsystems

The Certificate Management System is the core of the PKI. To provide flexibility in a PKI, the CMS instance can be configured as one of four possible subsystems.

- Certificate Manager (CA) serves as the Certificate Authority for the PKI. A CA instance can be configured as either a Root CA that creates a self-signed certificate or a subsidiary CA that requests a signing certificate from another trusted CA. The CA provides "functionality for issuing, renewing, revoking, and publishing certificates and creating and publishing Certificate Revocation Lists (CRLs)."[31]
- Registration Manager (RA) is used for user verification and certificate request approval. Approved requests are then sent to the CA for certificate creation using a trusted certificate issued by the CA.
- Online Certificate Status Manager (OCSM) is used as an Online Certificate Status Protocol (OCSP) service "for real-time verification of certificates issued by the Certificate Manager."[32]
- Data Recovery Manager (DRM or KRA) provides encrypted storage for private keys and facilitates their recovery.

4. Nuts and Bolts

The CMS itself is a set of "pure JAVA classes"[33]. Each subsystem is installed and configured with HTTP servlets to enable subsystem services. The default installations of all of the subsystems can be enhanced using configurable JAVA plug-ins. These modules (JAVA plug-ins) can be used to configure a variety of services including:

- Access Control Lists
- Authentication

---

[29] Netscape Communications Corporation, "Administrator's Guide Netscape Directory Server," [http://enterprise.netscape.com/docs/directory/61/ag/intro.htm#1043886], August 2002. Accessed June 2004.

[30] Netscape Communications Corporation, "Administrator's Guide Netscape Certificate Management System Version 6.1," February 2003. (Administrator's Guide)

[31] Administrator's Guide, p. 30.

[32] Ibid., 167.

[33] Ibid., p. 58.

- Authorization
- Logging
- Job schedule
- Publishing
- Email notification
- Event listeners

The diagram (Figure 4) below is the architecture of the CMS. The rest of this chapter will go into more detail about the specifics of the CA, RA, and KRA subsystems used in the PKI, how they communicate with each other and the processes used for the certificate life-cycle.

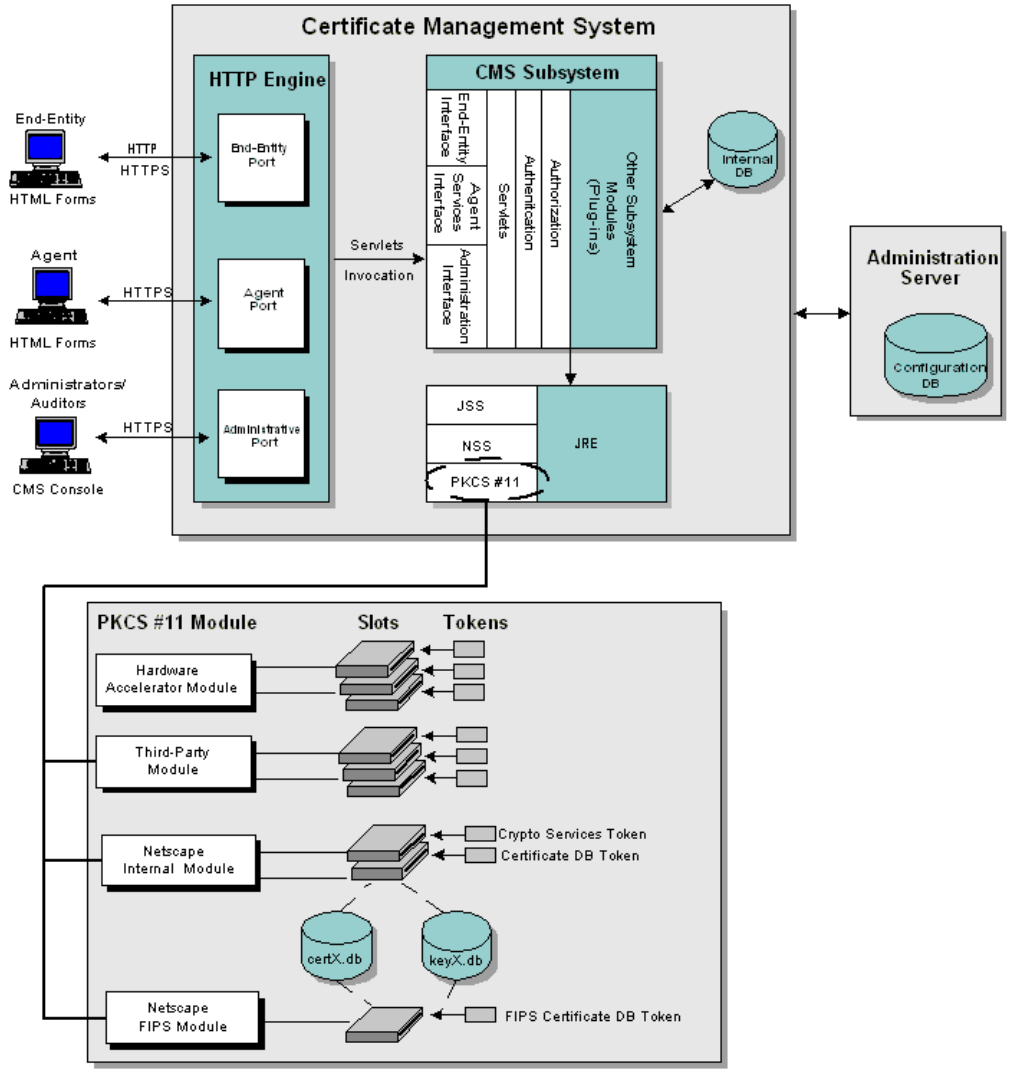


Figure 4. CMS Architecture[34]

a. HTTP and JAVA Servlets

Though CMS is built on the foundation of JAVA classes, other programming languages and services are needed to complete the functionality. A key aspect of communication with the subsystems by users and agents is the HTTP engine. This service is provided by the Netscape Enterprise Server that "delivers static and dynamic Web content". Netscape Enterprise Server supports "most current standards including HTTP 1.1, SSL, PKCS#11, and LDAP" and provides both content and

[34] Ibid., p. 58.

functionality of the non-SSL and SSL end-entity web interfaces and the agent's SSL web interface. While these interfaces will be described in depth in the Functionality section of this chapter, the HTML pages are enhanced, their content created, and requests processed by the JAVA servlets. Each subsystem has specific servlets for their purposes. The OCSM and the CA's OCSP responder use JAVA servlets to respond to OCSP requests.

b. NSS

"Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled communications applications."[35] NSS helps make the SSL client authentication and other secure communications between subsystems work.

c. JSS and the JAVA/JNI Layer

The Java Security Services (JSS) is the Java foundation for the Java interface with NSS. Built using the Java Native Interface (JNI), JSS allows for customizable services to be created for the subsystems. These services can then be successfully run by different versions of the Java Virtual Machine (JVM).[36]

d. PKCS #11

One of the keys to a successful PKI is strong cryptographic information. For this, the CMS uses Public-Key Cryptography Standard #11 modules which communicate with cryptographic storage devices. "The PKCS standards are specifications that were developed by RSA Security in conjunction with system developers worldwide (such as Microsoft, Apple, Sun etc.) for the purpose of accelerating the deployment of public key cryptography." [37]

The CISR PKI uses the Internal Crypto Services token used by each subsystem to perform cryptographic operations. Another benefit of CMS is that it also comes with the FIPS (Federal Information Protection Standard) 140-1 compliant module.

---

[35] Ibid., p. 62.

[36] Ibid., p. 61.

[37] Mohan Atreya, "Introduction to PKCS Standards," [http://www.rsasecurity.com/products/bsafe/overview/IntroToPKCSstandards.pdf#xml=http://www.rsasecurity.com/programs/texis.exe/webinator/search/xml.txt?query=pkcs+%2310&pr=default_new&order=r&cq=&id=40c6e13bb], 2004. Accessed June 2004.

FIPS 140-1 is an "evaluation criteria associated with cryptographic modules."[38] The default model of the CMS is not DoD compliant, further research should be done using FIPS 140-1 to ensure compliance with DoD standards.

e. Command Line Tools

For those users more comfortable with command line operations and to allow for greater customization, Netscape has provided a variety of command line tools for CMS management. They include certutil, a backup/restore tool, a password cache tool and a mass revocation tool to name a few. Certutil, or the Certificate Database Tool, "is a command-line utility that can create and modify the Netscape Communicator cert7.db and key3.db database files."[39] For CMS, these files are maintained in the internal token and are used to validate certificates the CMS receives.[40] The CMS Software Development Kit (SDK) can also be used for customization and tutorials for use with command line tools and other functions of the CMS.

C. INSTALLATION ISSUES

During the conduct of this research, several issues arose during the installation of the CMS software on the NPS Sun machines. CMS 6.1 currently has two versions one for Solaris 8 and one for Windows NT. The selection of the Sun Blade 100s dictated that the version for Solaris 8 was used. Unfortunately, the Sun boxes had been previously configured with hardened security features for the Cyber Defense exercise and were running Solaris 9. These security features caused the initial installation attempts to fail miserably. The solution was to reformat both boxes and begin with fresh installation of Solaris 8. Once a successful installation was completed, the decisions turned to the deployment scheme of the PKI.

The second issue was the limitation of the hardware. Figure 5 is the preferred deployment scheme of a PKI, one host for each of the three subsystems, a Certificate Manager, Registration Manager, and Data Recovery Manager.

---

[38] Carlisle Adams and Steve Lloyd, "Understanding PKI, 2nd Edition," Addison Wesley, 2003.

[39] The Mozilla Organization, "Using the Certificate Database Tool," [http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html], December 2002. Accessed June 2004.

[40] Administrator's Guide, p. 294.

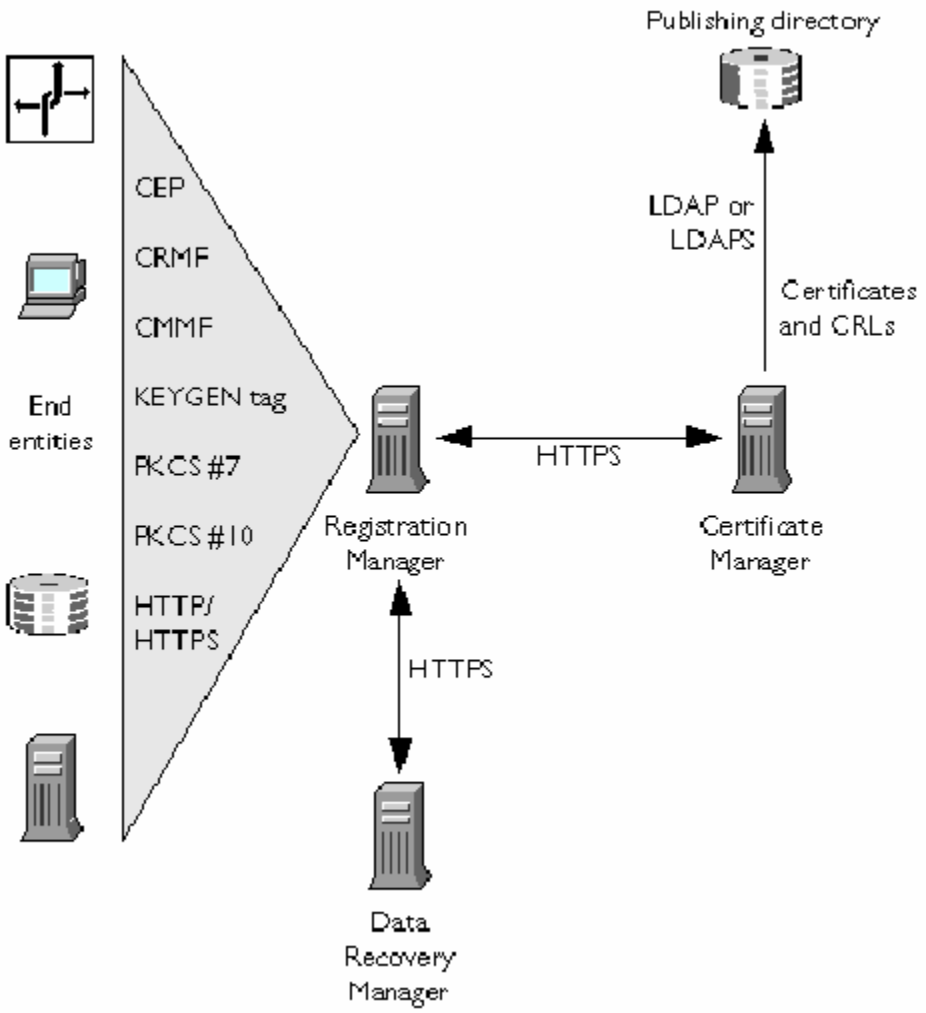


Figure 5. Certificate Manager, Registration Manager and Data Recovery Manager in Separate Instances.[41]

Unfortunately with only two machines available in the NPS CISR lab to support this project, an alternate (non-optimal) solution was adopted.

As discussed above, the CMS software contains an administration server, a directory server and a CMS server. Each server is referred to as an instance in the Netscape Console which is a graphical user interface (GUI) used to configure and control the Netscape servers. One instance of each of the three servers is installed in a server group during the initial setup. Netscape allows for two configurations if multiple CMS instances are required on one machine. First, one server group can be installed and then

[41] Ibid.

multiple CMS instances can be added to the group. Second, multiple server groups can be installed each with their own set of three servers. The deployment scheme chosen for the CISR PKI included a root CA, a RA and a KRA or Data Recovery Manager (DRM is used by Netscape to refer to a KRA). With only two computers, the decision was made to place the CA and KRA on one machine and the RA on the other. The CA was setup first in the server group and then a second CMS instance was created and setup as the KRA as shown in Figure 6. The problem arose when trying to start the KRA instance.

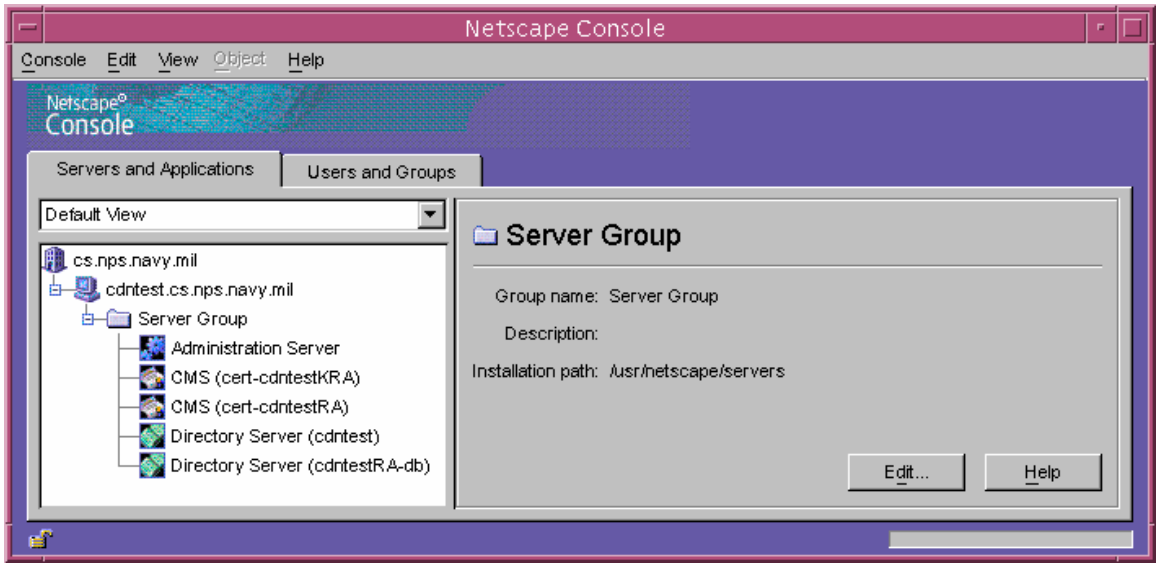


Figure 6. One Server Group with Two CMS Instances.

Only one CMS instance would run at one time in the server group. This deployment scheme was scrapped and a second deployment option for multiple server groups was used for the future installations (Figure 7). Multiple server groups allowed both CMS instances to function concurrently with no failures to start the KRA instance.

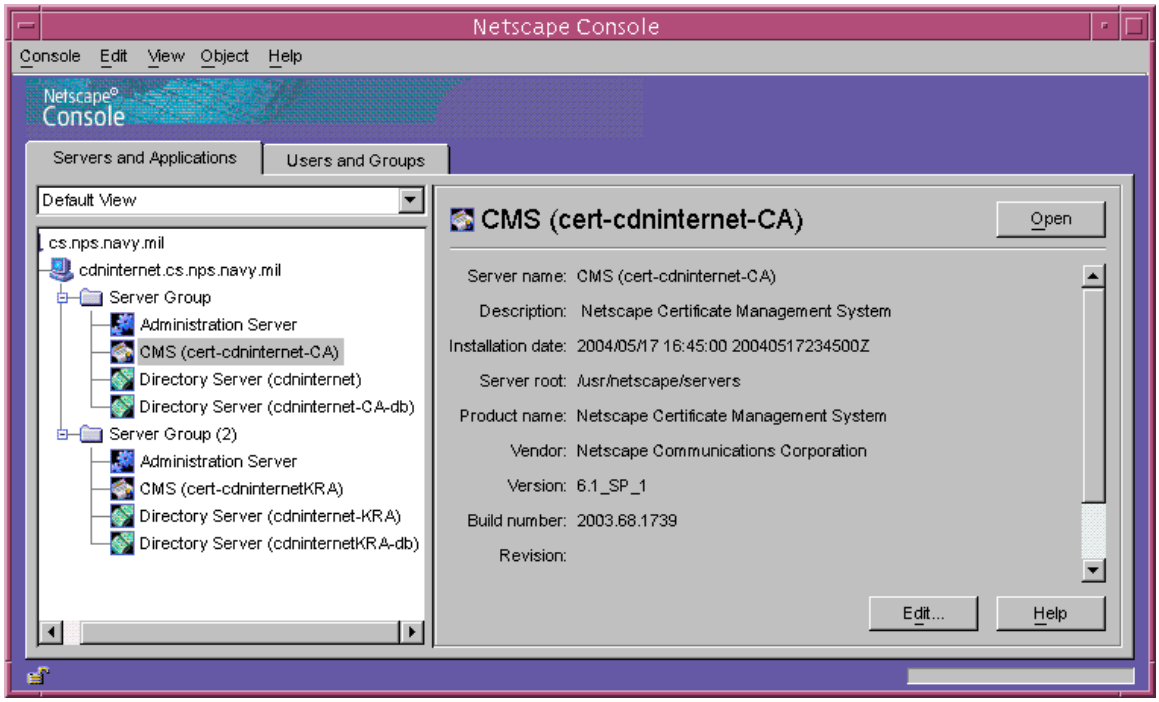


Figure 7. Multiple Server Groups

The initial project envisioned an OCSM instance to provide OCSP services. When attempting to add an OCSM to the above deployment scheme, another issue developed. The not enough disk space error was received. The routine solution to this problem is to reformat the hard drive, reinstall the operating system and repartition the disk space to accommodate the software. Not wanting to remove all of the work successfully completed, another alternative was tried. A second hard drive was installed in the computer and the essential partitions were copied to it once they were checked for errors. Once this was completed, the format command was used to repartition the first hard drive, increasing the root partition to 5 Gigabytes. With repartitioning complete, the data saved on the second hard drive was then dumped back to the first hard drive. These steps were then repeated for the second machine. Once the repartitioning was accomplished, no future issues occurred because of disk space.

D. FUNCTIONAL OVERVIEW

The CMS operates using a combination of many different languages and types of files. This section will discuss some of the specific files and interfaces used for the operation and configuration of the CMS PKI. The majority of the configuration

information used by the Administration Server are located in the config directory of the CMS instance. This information is what is seen through the Administrative Interface and used to perform the tasks of the subsystem.

1. Interfaces

There are four interfaces that allow users to communicate with a CMS subsystem, the Non-SSL and SSL end-entity interfaces, the agent interface, and the administration interface also called the Netscape Console.

a. Administrative Interface

Each subsystem is managed through the Netscape Console and Administration Server, also known as the Administrative Interface. "Based on the information given at each command, the administration servlets allow administrators to perform administrative tasks and configure plug-in modules and instances of plug-in modules."[42] The interface is similar for all of the subsystems, but provides different functionality for each. For instance, the DRM has a section for changing recovery agent information that the other subsystems do not have.

Although the Administrative Interface is only accessed through Netscape Console (Figure 8), there are a few HTML pages and templates that are used for the initial agent enrollment. The adminEnroll.html page allows the CA agent to create a request for a certificate and the EnrollSuccess.template and ImportCert.template display the newly created certificate and allow for it to be imported into the browser. This certificate is also added to the user that was created as an administrator during the configuration of the CMS instance. The Initial Agent Enrollment is only available on the CA because there are agents to approve requests. Once the agent is created, other subsystem agents can go to the CA with their certificate requests. These HTML files are located in the agent subdirectory of the web-apps directory of the CMS instance and are disabled after the initial agent has been enrolled.

[42] Ibid.

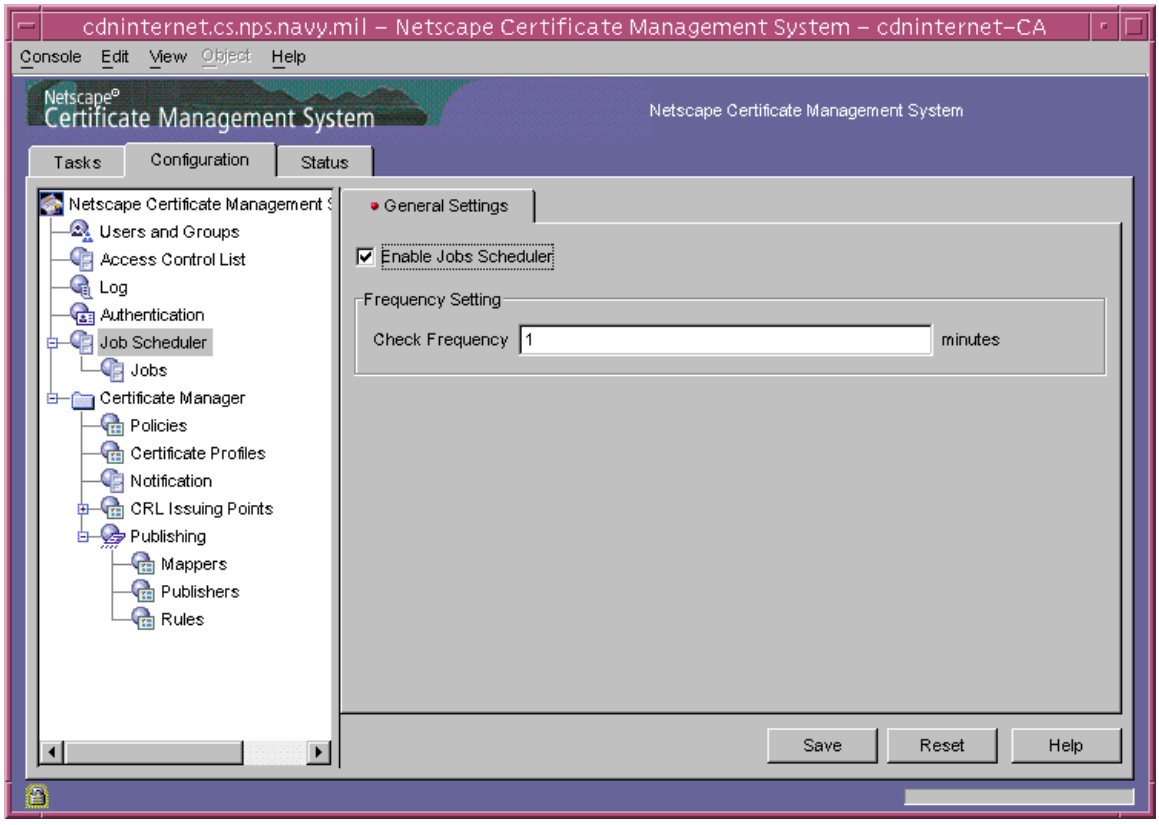


Figure 8. A View from the Netscape Console that Controls the CA.

b. Agent Interface

The Agent Interface is used by agents of the subsystem to perform specific tasks relating to that subsystem. For the CA and RA, these activities consist of the following: approving/disapproving certificate profiles, approving certificate requests and certificate renewals. The CA is the only subsystem that has the controls for CRL creation and issuance. The DRM's agent interface is used specifically for approving key recovery requests and locating keys. For the OCSM, the interface is used to control responses to OCSP requests and CRL retrieval and storage.

The agent interface is created using a combination of HTML files and templates that use JavaScript functions to populate the information that appears in the web browser. These files are maintained in the agent directory of the web-apps directory in the CMS instance directory. The agent directory contains subdirectories for each

possible subsystem although only the files relevant to the particular instance are used. They can be modified to display only that information necessary for a particular PKI deployment.

c. Non-SSL and SSL Interface

The end-entity interface allows for end-user communication with the CA, RA, and OCSM. The end-entity page can be accessed either by http or securely on https using SSL. A certificate is used to authenticate the user to the SSL for secure communications. For the CA and RA, the interface includes:

- an enrollment tab with access to certificate profile forms
- a revocation tab for user revocation, and
- a retrieval tab where users can download their certificates and import the CA chain.

The CA has added functionality in that users can list certificates and download the current CRL. The end-entity interface of the OCSM is for acceptance and processing of OCSP requests via JAVA servlets. The DRM does not have any end-entity interfaces.

Both the Non-SSL and SSL end-entity interfaces are also created using a combination of HTML files and templates (Figure 9). The JavaScript functions provide information and allows for authentication and access to the SSL end-entity interface. The HTML files for the certificate enrollment profiles are also stored here. The options that appear in the key generation request type and request fields are determined based on the JavaScript functions in the ProfileSelect.template and the owner's web browser. These files can also be modified to permit access to only required areas or to increase functionality. For example adding a renewal tab to the screen that provided access to the certificate renewal pages would facilitate owner certificate renewal. The files used for these interfaces can be found in the ee directory of the web-apps under the subdirectory associated with the subsystem.

Figure 9. Screen Shot of the SSL End-Entity Interface of the RA.

2. Users and Groups

Access to the administration and agent interfaces are controlled by registered users and their associated groups. By default, the Administrators, Agents, Auditors, and Trusted Managers groups are created for the CA. As their names describe them, members of the Administrators and Agents groups have full access to those interfaces respectively. Auditors have access to view signed audit logs only. Trusted Managers is the group that holds information about other subsystems that are registered as users of the CA such as the Registration Manager or a subsidiary CA. When a Trusted Manager is added as a user, the fully qualified domain name must be used as the full name of the user to allow recognition by the subsystem. Users can be assigned to one or more of these groups as required. In order to authenticate securely each user must have a certificate associated with it. More will be discussed about Trusted Managers in the Connecting the Subsystems section. Figure 10 shows the window used to import such a certificate. Users and Groups can be added, modified, or deleted via the Users and Groups tabs that appear when Users and Groups are selected in the left-hand portion of the Netscape Console.

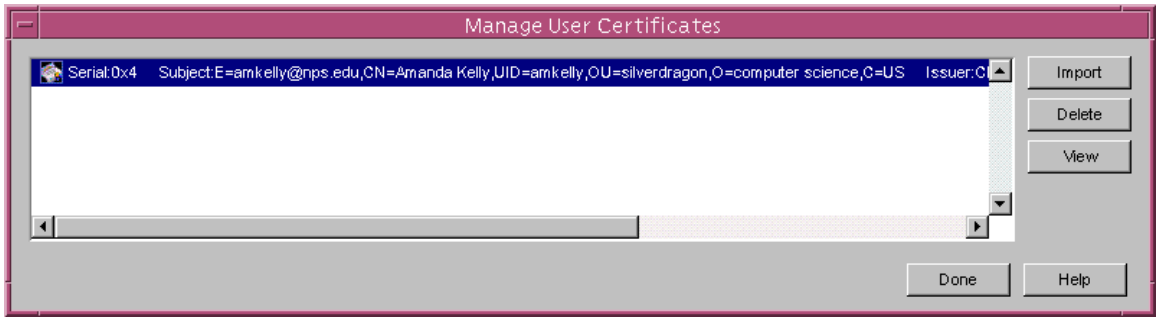


Figure 10. Certificates Associated with a Specific User

User and Group information is stored in the Directory Server instance created during the configuration of the CMS subsystem.

3. Connecting the Subsystems

In order for the PKI to work correctly there must be a trust relationship between the subsystems. The Netscape CMS uses connectors, the Trusted Managers group, and certificates to establish these trusted relationships. Via the console, the CA has the ability to connect to a DRM or an OCSM. The RA has the ability to connect to a DRM and a CA. The connector must be enabled and requires the host name, port number, and a timeout limit. The subsystem must be a user assigned to the Trusted Managers Group of the subsystem to which it is trying to connect. For example, for communication between a RA and CA to succeed, the RA must be a user in the CA's Trusted Managers Group. On the DRM, the CA user must have the CA SSL certificate associated with it. The RA must have its signing certificate associated. On the CA, the RA user must have a matching signing certificate associated with that user. Below is a snapshot of the information for a connector in the console (Figure 11).

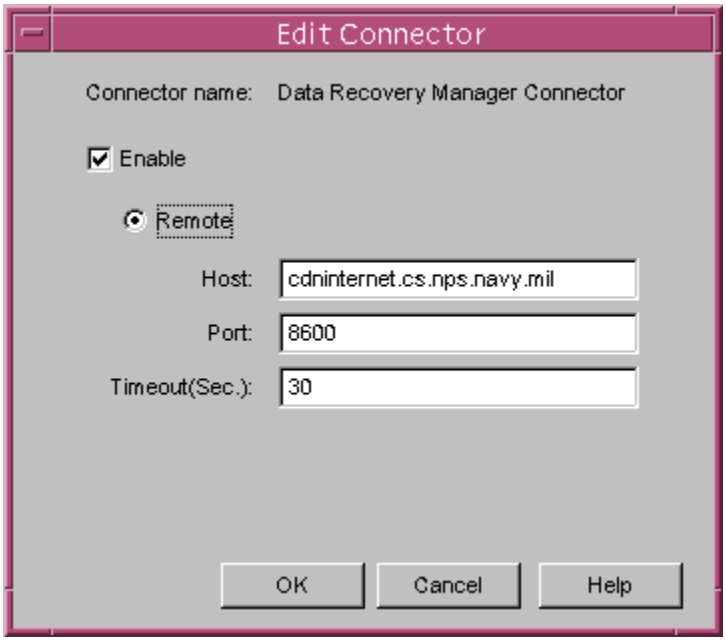


Figure 11. Information Associated with a Subsystem Connector.

The next aspect of connecting the DRM with the CA and RA involves imbedding the DRM transport certificate into a JavaScript function in the ProfileSelect.template used to create the html pages used for certificate enrollment profiles via the end-entity interfaces. Below are the functions used to generate and send the Certificate Request Message Format (CRMF) to the KRA. For simplicity, the majority of the 64-base encoding for the keyTransportCert of the KRA has been deleted.

```
function validate()
{ if (keygen_request == 'false')
        return false;
        with (document.forms[0]) {
        var keyTransportCert = "MIIDlzCCAn+gAwIBAgIB0Bw0=";
        // generate keys for nsm.
        if (typeof(crypto.version) != "undefined")
                { if (dual == 'true') {
                  crmfObject = crypto.generateCRMFRequest(
                  "CN=x",
                  "regToken", "authenticator", keyTransportCert,
                  "setCRMFRequest();",
                  1024, null, "rsa-ex",
                  1024, null, "rsa-sign");
                } else
                  { crmfObject = crypto.generateCRMFRequest(
                    "CN=x", "regToken", "authenticator",
```

```
                    keyTransportCert, "setCRMFRequest();",
                    1024, null, "rsa-dual-use");
                }
        } return false;
}
}
function setCRMFRequest()
        { with (document.forms[0])
          { cert_request.value = crmfObject.request; submit();
        }
}
```

The web browser that is used by the owner during the certificate request phase must support the creation of dual key pairs, one private and one public. Netscape 7.1 is currently the only browser that allows this to be done via a CRMF request. Microsoft's Internet Explorer uses an internal cryptographic provider for the key generation and storage, although a CRMF request should still travel to the KRA.

The final step is ensuring the DRM trusted the certificate chain of the CA. This is done from the Netscape Console for the DRM under the encryption tab. The Manage Certificate button brings up a list of CA certificates, their expiration date and their trust status. First the CA certificate must be in this list and second the certificate must be trusted. This information is maintained in the Directory Server installed during the configuration of the DRM subsystem. Figure 12 shows the trust relationship as seen in the Manage Certificate window of the RA. The CA trust relationship must also be setup in the RA.

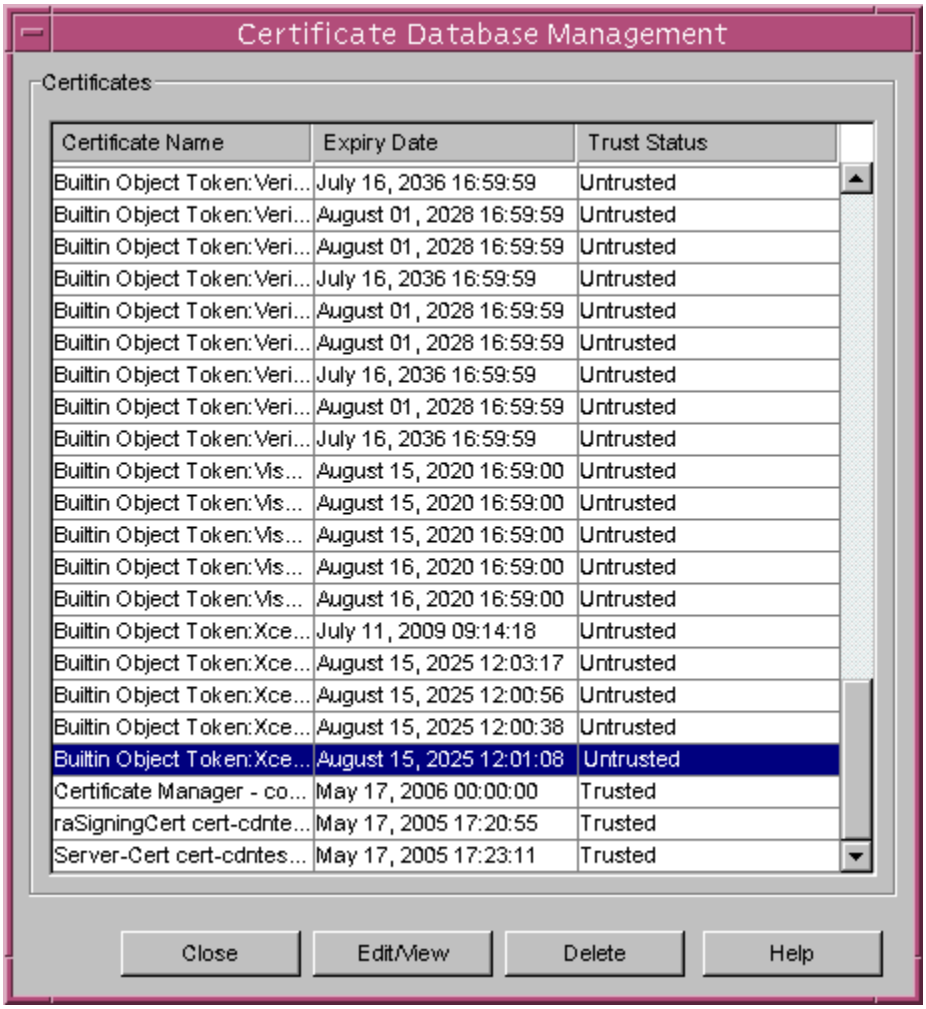


Figure 12. Manage Certificates Window

At the time of writing, there is still an error in the trust relationship between both the RA and CA, and the DRM. There is a creation of a CRMF request during the certificate enrollment process, however there is no sign of it after the request has been sent to the CA. One possible solution would be to request new certificates for the RA and DRM using the Certificate Setup Wizard that directly imports the certificates into their locations in the Directory Server. Perhaps there was an error in the generation of keys during the CMS configurations that prevented proper functionality.

4. Certificates

Creating and distributing certificates are core functions of a PKI. Certificate enrollment can be initiated from several different locations, the Non-SSL and SSL end-entity interfaces and the Certificate Setup Wizard in the Administrative Interface of a

subsystem. This section will discuss all the various processes involved throughout a user certificate's life-cycle. Subsystem certificates are created using the Certificate Setup Wizard and request approval via the agent interface of the CA. This wizard is accessed via the Netscape Console of the subsystem and is discussed in detail in the Appendix.

a. Certificate Enrollment

- The owner opens a browser window to one of the end-entity pages of the RA.
- The owner selects the Certificate Profile he wishes to use, enters the information requested, and clicks submit.
- The web browser then generates the dual (public and private) key pair. In Microsoft Internet Explorer the keys are stored in one of the Cryptographic Providers. In Netscape, the keys are stored in the Software Security Device.
    - Internet Explore generates a PKCS #10, a type of message format for certificate requests from RSA Securities, and sends the request to the RA.
    - Netscape generates a CRMF, a type of message format used to convey certificate requests proposed by the Internet Engineering Task Force (IETF) PKIX working group, and sends the request to the RA.
- The request is evaluated against existing profiles and accepted or rejected.
- A RA agent using the agent interface views the certificate request, makes any change necessary, and the approves or disapproves the request.
- Once approved, the RA signing certificate is used to sign the request and the RA agent then forwards it to the CA.
- The CA compares the request against its own profiles and if nothing is violated, it generates the certificate.
- If key archival is requested, the certificate and the key pair are transported to the DRM, and signed by the DRM's transport certificate.
- An email is then sent by the CA to the certificate owner containing a link to the retrieval page.
- The owner then imports the certificate into his browser and is ready to go.

Certificate requests and certificates are stored in the Directory Server instance created during the subsystem installation. The CA can also publish certificates to this directory to enable ldap retrieval of the certificates.

b. Certificate Renewal

- The Job Scheduler of the CA processes the Certificate Renewal Notification Job, discussed later in this chapter, and sends an email to the certificate owner.
- The certificate owner follows the link in the email to the SSL end-entity page of the RA and the Renewal Page.
- At the Renewal Page the owner click Submit (Figure 13).

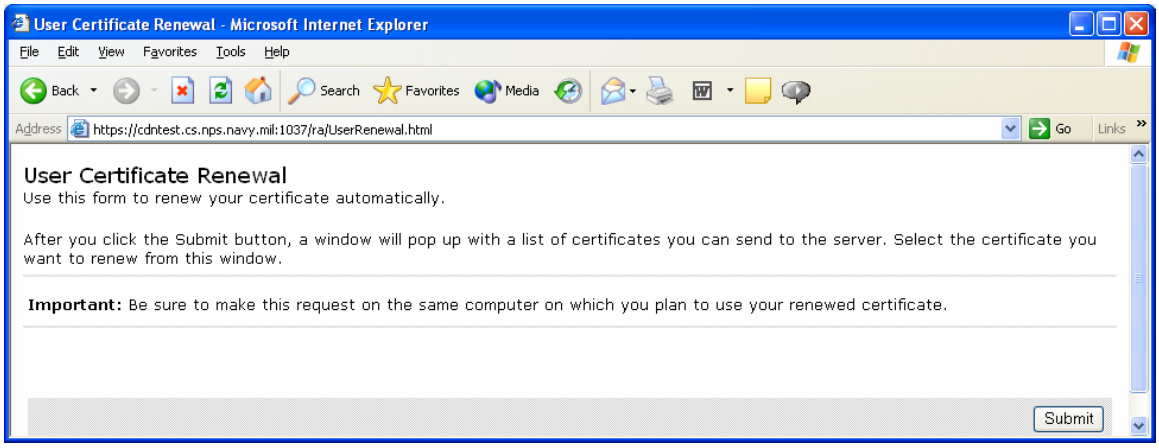


Figure 13. Certificate Renewal Page

- A selection window then appears with a list of certificates available. The owner selects the certificate she wishes to renew and clicks ok.
- The request is sent to the RA, which signs the request and forwards it to the CA.
- The CA evaluates the request against its profiles and issues the certificate if all is in compliance with policy.
- The certificate is then imported into the owner's browser.

c. Owner Certificate Revocation

- The certificate owner clicks on the Revocation tab of the RA's SSL end-entity page (Figure 14).

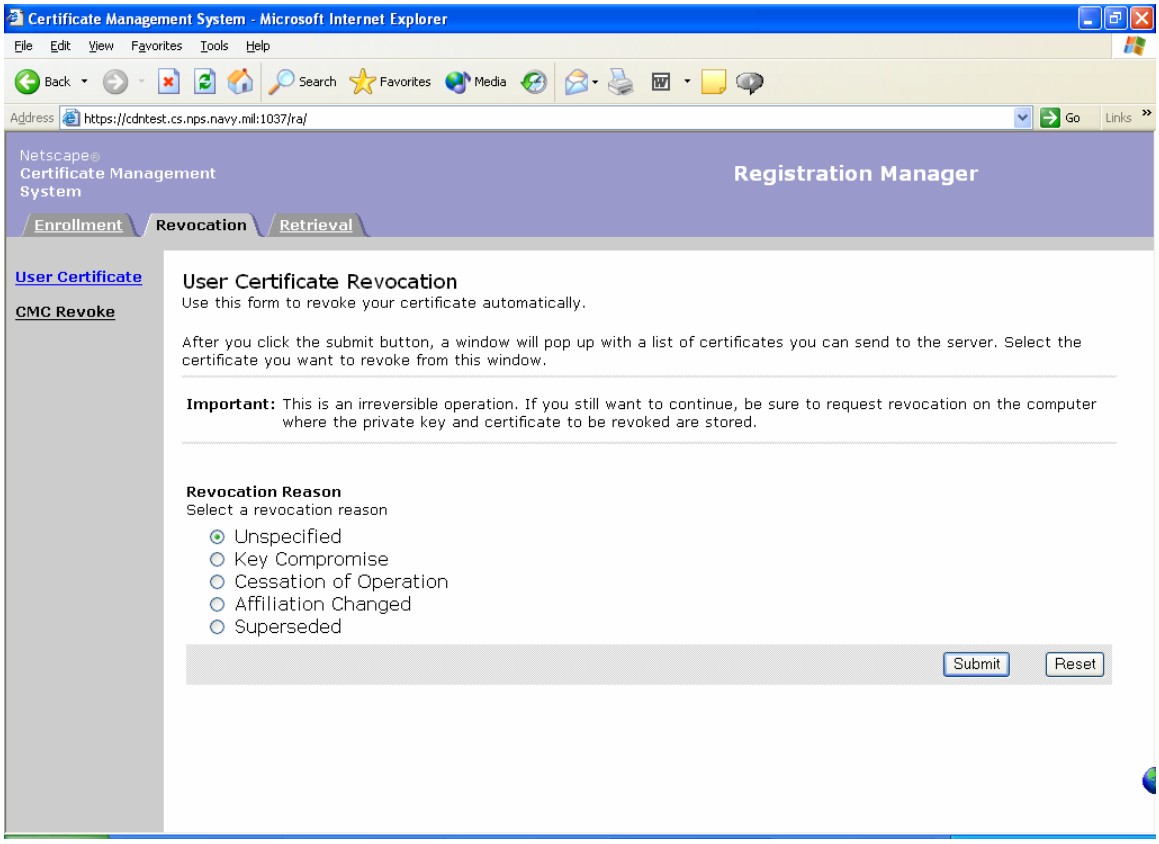


Figure 14. SSL End-Entity page for Certificate Revocation.

- The owner selects the revocation reason and clicks Submit.
- The browser prompts her to select the certificate she wishes to revoke.
- The Certificate Revocation Confirmation page appears, with the details of the certificate chosen and the opportunity to add comments.
- Since the RA is does not have the authority to revoke certificates, the request is forwarded to the CA.
- The certificate is revoked by the CA by marking as such in the database (Directory Server), the CRL is updated with this new revocation, and it is published to the Directory Server. An email is also sent to the owner confirming that the certificate has been revoked.

d. Agent Revocation

Agent Revocation is similar to owner revocation, but it can only be performed through the agent interface of the CA. The RA does not have the authority to revoke certificates as mentioned above.

- An agent of the CA opens the agent interface of the CA.
- There are two possible ways to revoke a certificate from here.

- Select List Certificates and navigate to the certificate you wish to revoke.
- Batches of certificates can be revoked by entering qualified parameters, such as validity dates or all certificates approved by a specific person, via the Revoke Certificates page.

- A Certificate Revocation Confirmation page will appear where the agent selects the revocation reason, an invalidity date if needed, and additional comments. The agent then clicks Submit.
- The certificate is then marked as revoked in the database, an email is sent to the certificate owner, and an updated CRL is published.

5. Jobs and Notifications

The CMS uses email alerts to notify certificate owners of successful certificate request processing and certificate renewal and revocation. Alerts to an agent can also be enabled providing the agent with information about certificate requests in queue and summaries of renewal notifications that have been sent. To enable these emails to be sent, an SMTP connection must be enabled in the Netscape Console including the server name and port number. These alerts are split into two categories: jobs and notifications.

a. Notifications

The CA has three default notifications, Certificate Issued, Certificate Revoked, and Request in Queue. Since the RA lacks the ability to revoke a certificate, this notification is not available from the RA. Each notification can be enabled or disabled and assigned a different sender (Figure 15). Each also has a default template stored in the email directory of the CMS instance directory. The templates, certIssued_CA.html for example, can be modified to include information relevant to a particular PKI deployment. The Request in Queue notification can be setup through a comma delineated list to send to multiple RA or CA agents.

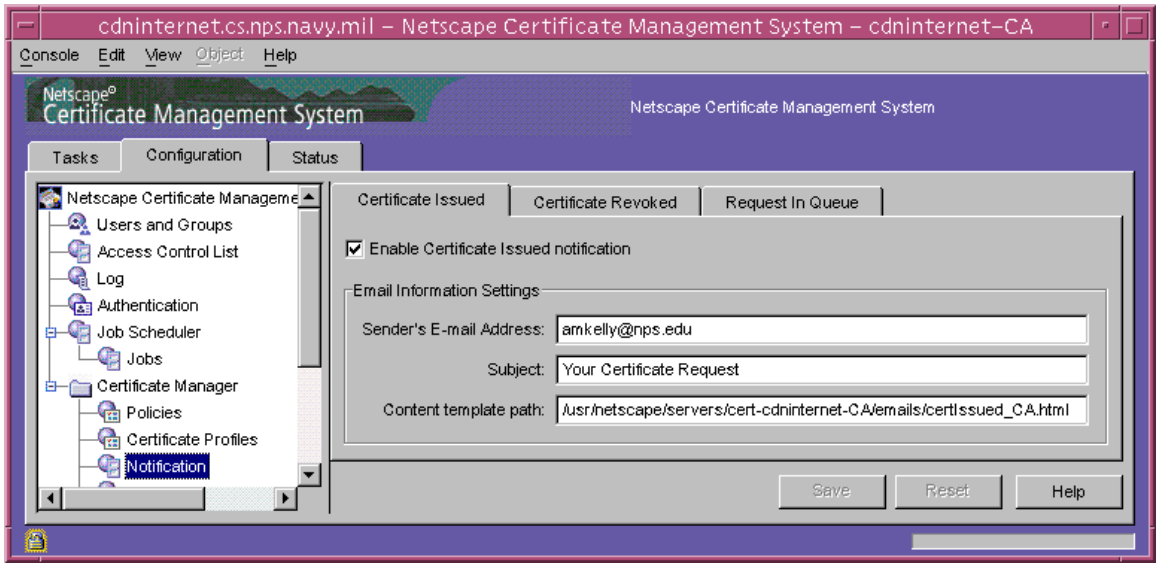


Figure 15. Notification that Can Be Enabled in the CA.

b. Jobs

Jobs are executed using the Job Scheduler, which is setup to check the configuration of job instances and execute them at a specific time. The CA is installed with a renewal job, a request in queue job, and an unpublish expired certificates job. These jobs can be configured to execute based on five criteria: minute, hour, day of month, month of year, and day of week. Figure 16 shows some of the other areas that can be configured on a job.

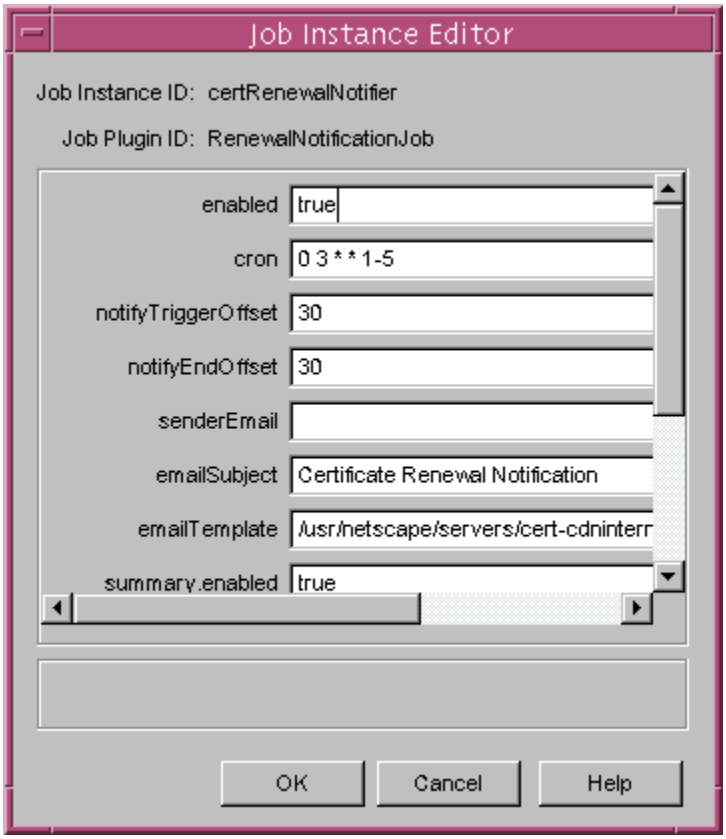


Figure 16. Job Instance Editor for the Certificate Renewal Job

Each job instance refers to an email template that can be configured to provide specific information for an organization. An agent can create and register custom job plug-in modules and job instance using the modules via the Netscape Console.

6. CRL and Publishing

One of the problems that arise in the implementation of a PKI is keeping track of revoked certificates. The CMS CA has an internal OCSP responder that checks the certificate database to determine if a certificate is valid; however other applications require a Certificate Revocation List against with to verify certificate validity. The CA has the ability to publish CRLs to several different issuing points. An Issuing Point is "a location where a subset of all the revoked certificates are maintained."[43] It is also an entry in the Directory Server enabled for LDAP communications. For the purposes of this research, the CRL was published to the MasterCRL (Figure 17) and LDAP publishing was enabled via the Directory Server.

[43] Ibid., p. 601.

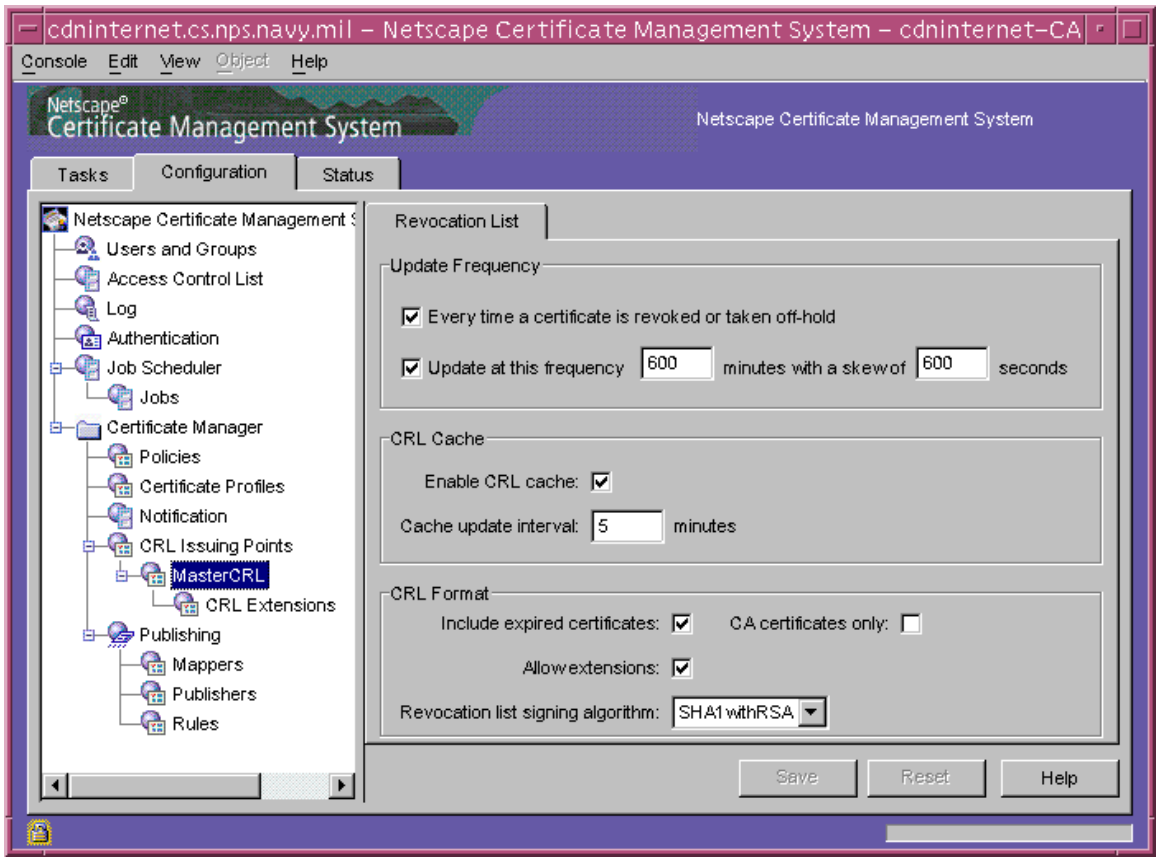


Figure 17. MasterCRL Configuration in CA's Console

Each CRL Issuing Point, like the MasterCRL, has CRL extensions associated with it. These can be enabled or disabled based on the implementation. They include:

- CRL Reason - reason for the certificate revocation
- Invalidity Date – date the certificate is invalid
- CRL Number – number of the CRL
- Issuing Distribution Point – the location of the CRL

As seen in Figure 17, there are a variety of settings that can be set for each issuing point. An administrator can setup one issuing point that only issues CRLs for CA certificates and another issuing point that only issues CRLs about user certificates.

Publishing must be enabled to be able to publish a CRL to a directory for LDAP download (Figure 18). The Mappers, Publishers, and Rules seen in Figure 16 provide configuration information about the location and policies for LDAP publishing. With

publishing enabled, the CRL is then saved to an Issuing Point location in the database and can be pointed to in the CRL Distribution Point certificate extension for certificate validation purposes.

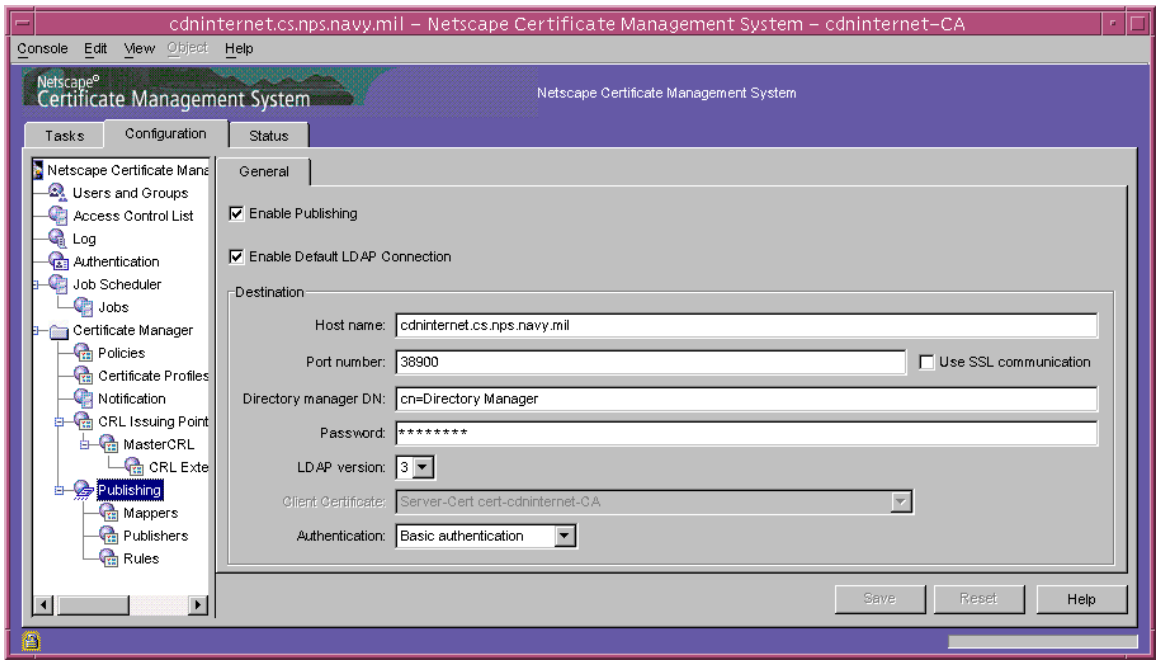


Figure 18. Publishing Enabled on the CA

7. Certificate Profiles

> A certificate profile defines everything associated with the issuance of a particular type of certificate including the authentication method, the certificate content (defaults), constraints for values associated with that content that can be contained in this type of certificate, and the contents of the input and output forms associated with the certificate profile.[44]

Certificate profiles are created, modified, and deleted through the administrative interface of the CA and RA (Figure 19); however, they are approved and disapproved for end-entity use through the agent interface. From the agent interface of the RA or CA, **Manage Certificate Profiles** is selected. A profile is then selected from the list of certificate profiles that have been created for the subsystem. From this web page, profiles are approved or disapproved for publication to the end-entity interfaces. In order to make modification to a certificate profile, it must be disapproved.

[44] Ibid., p. 431.

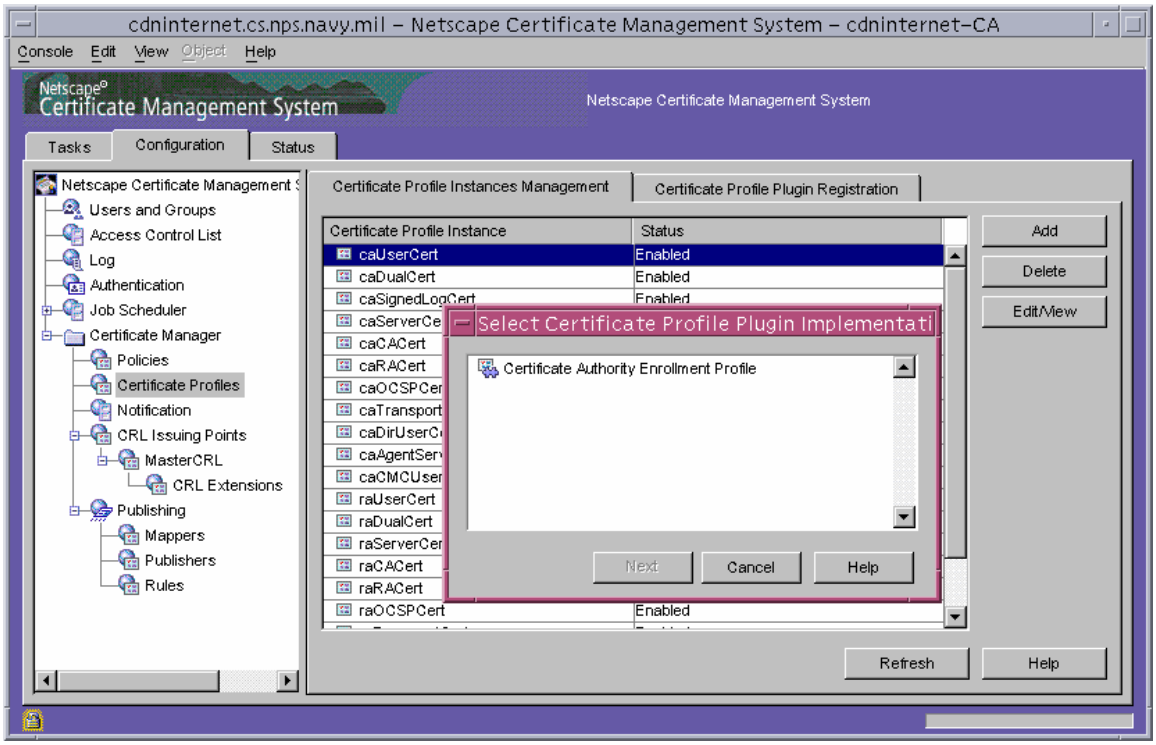


Figure 19. Certificate Profile Instance List and Plug-in Selection for a New Profile

Profile instances are maintained via the Administrative Interface. From there they can be added, deleted, viewed, and modified. Each certificate profile contains certificate extensions required, inputs, and outputs for the certificate. Constraints and specific information relating to an extension are also controlled here (Figure 20).

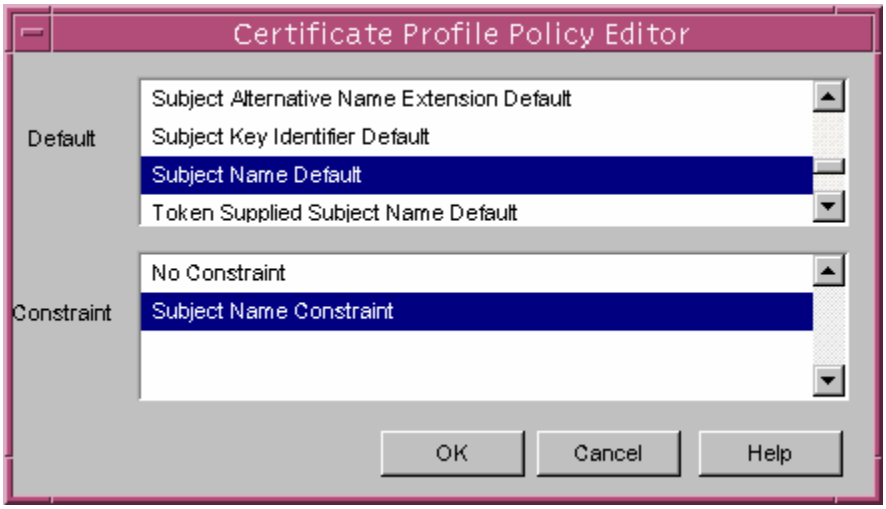


Figure 20. Certificate Profile Policy Editor for Certificate Extension Addition

In order for a certificate to be created using a profile on the RA, the profile must also exist on the CA. On the RA, the box, **End User Certificate Profile,** must be set to true (Figure 21).

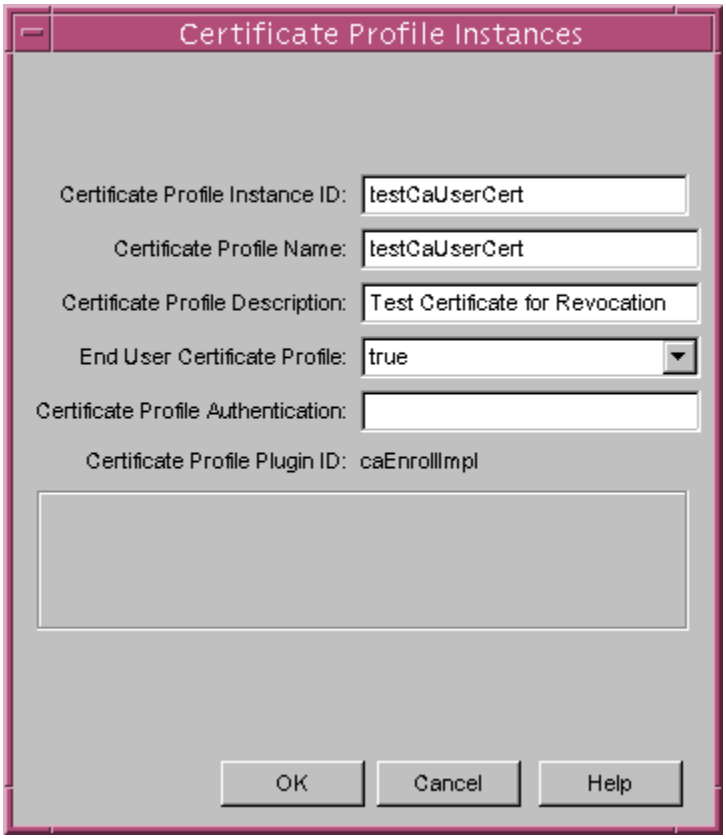


Figure 21. Creation of Certificate Profile Instance

On the CA, this box must be set to false so that the request is not processed through the associated input form of the CA. Each profile has a HTML file in the web-apps ee directory. Profile information is also stored in configuration files in the profiles directory of the subsystem, containing information to the certificate extensions and constraints required for the certificate. Profiles can be created for any use and multiple types of certificates can be issued for an organization based on a person's role in the organization.

8. Key Archival and Recovery

Key archival and recovery are another aspect of PKI implementation. Archiving a certificate owner's private key allows for him to recover the key if he accidentally deletes all of the key information associated with his certificate but he still needs to get to the information that he encrypted using his public key. Archiving also allows a company

to recover an employee's private key to decrypt files that he encrypted once he has left the company. This research was supposed to create a working model of the Key Archival (Figure 22) and Recovery process, however there was a problem with the trust relationship between the CA and the DRM that prevent successful implementation.

a. Key Archival

As discussed in the Connecting the Subsystems section, the transport certificate of the DRM is added to a JavaScript function in the ProfileSelect.template allowing the private key to be sent with the certificate request. The key is then stored in the internal token of the DRM encrypted using the DRM's storage key.

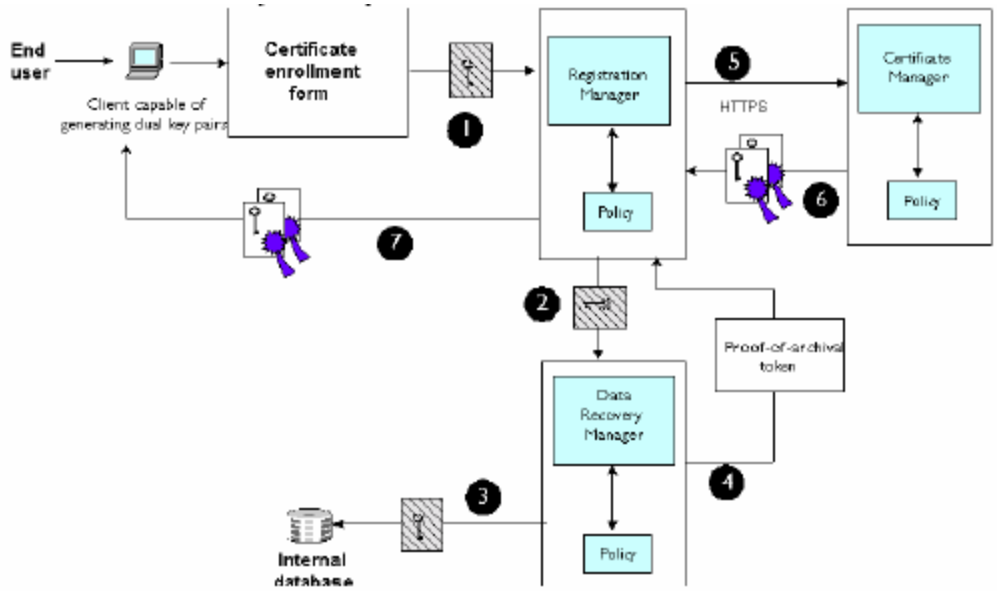


Figure 22. How the Key Archival Process Works[45]

b. Key Recovery

Archived keys remain encrypted until key recovery agents use passwords to unlock what is called password-splitting mechanism.

> For the protection of the storage key pair, the Data Recovery Manager supports a password-splitting mechanism called *m of n secret splitting or sharing*, whereby it splits the PIN that protects the token in which the storage key pair resides among *n* number of key recovery agents and

[45] Ibid., p. 203.

> reconstructs the PIN only if *m* number of recovery agents provide their individual passwords; *n* must be an integer greater than 1 and *m* must be an integer less than or equal to *n*.[46]

During the DRM subsystem installation, the administrator selects the m of n scheme, where m is the number of recovery agents required to unlock the storage key and n is the number of possible recovery agents (Figure 23).

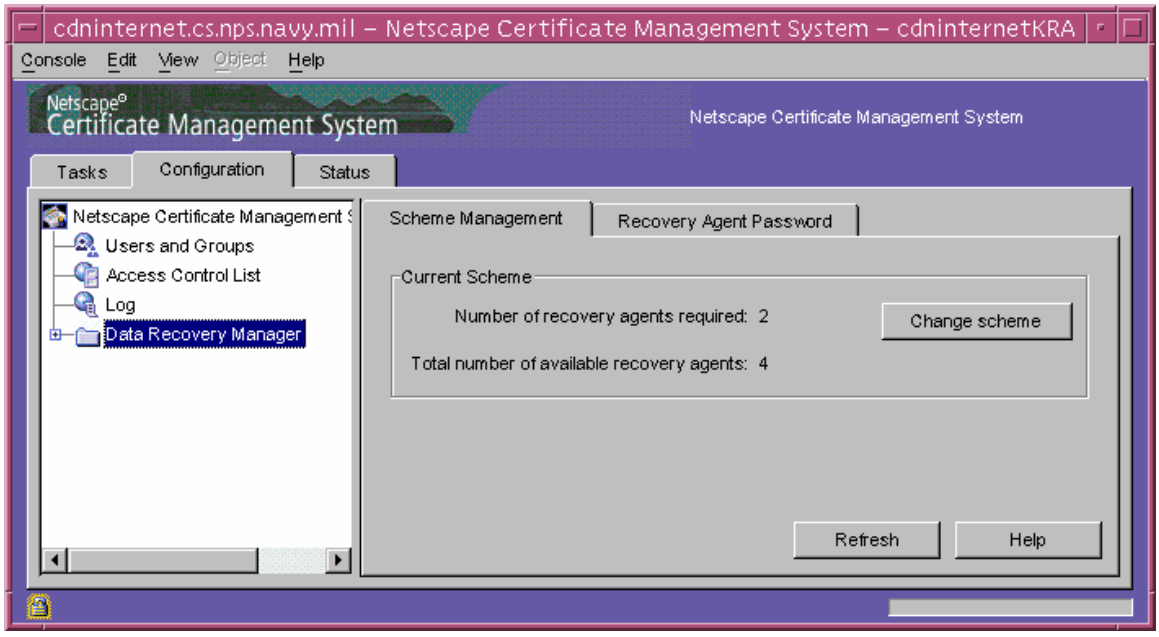


Figure 23. DRM Recovery Agent Scheme

CMS allows two types of Agent-Initiated Key Recovery Authorizations, local and remote. Local authorization requires the Key Recovery agents to be on the computer hosting the DRM. If the correct passwords are entered, via the agent interface, by m recovery agents, then the DRM retrieves the key and returns the key and its corresponding certificate in a PKCS #12 package. Remote Authorization is initiated by one recovery agent. Once the recovery request is initiated, the DRM sends an email with a specific reference number to all of the recovery agents. The required number of agents must individually access the DRM's agent interface and, using the reference number,

[46] Ibid., p. 206.

authorize the key recovery. The PKCS #12 package containing the key and its certificate are returned to the recovery agent initiating the request. Figure 24 shows the agent-initiated key recovery process.

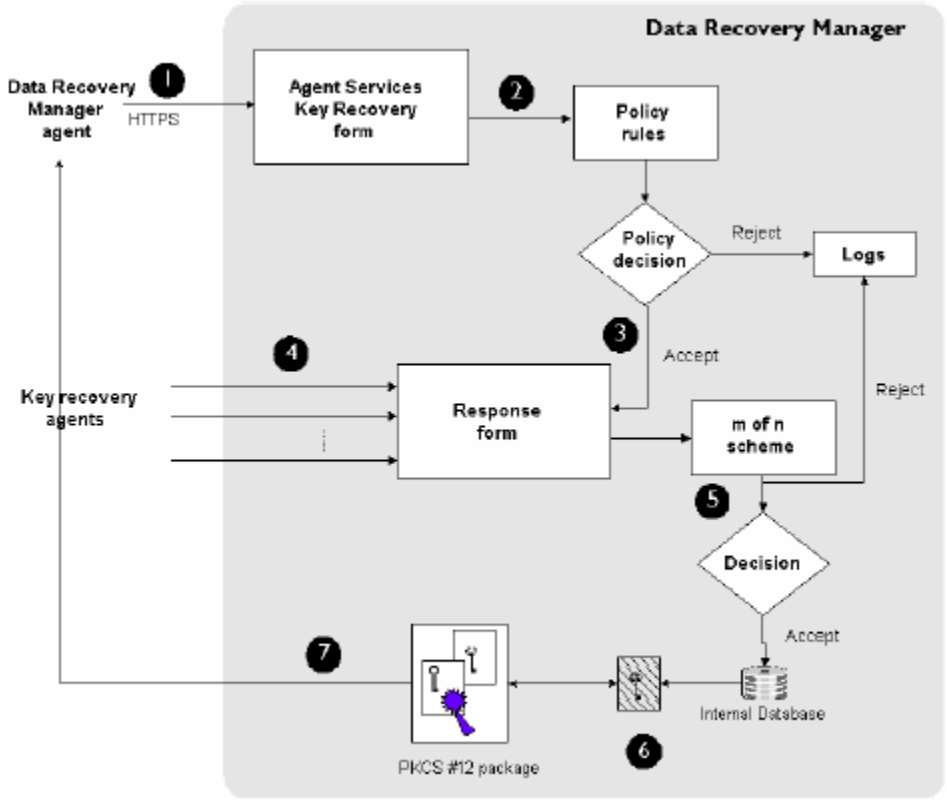


Figure 24. The Agent-initiated Key Recovery Process[47]

[47] Ibid., p. 209.

THIS PAGE INTENTIONALLY LEFT BLANK

V. VALIDATION OF CERTIFICATE LIFE-CYCLE FUNCTIONALITY

A. LIFE-CYCLE TEST SETUP

Installing and configuring a PKI does not necessarily mean that certificates can be created and used successfully for the purposes of confidentiality, integrity, authenticity, and non-repudiation. Testing of the PKI requires validation that all aspects of a certificate's life-cycle work. Certificates have essentially three phases, creation, use, and termination; either by revocation or by normal expiration. To test the functionality of this PKI, 20 certificates were taken through their life-cycle, with each being used to test one or more of the following functional requirements:

- Certificate Request
- Request Approval and Certificate Creation
- Certificate Download by Owner and User
- Certificate Use for Digital Signing of Email
- Certificate Use for Encryption of Email
- Normal Expiration of a Certificate
- Revocation for Cause (Administrative Action)
- Revocation by Owner
- Certificate Renewal
- Certificate Revocation Checking
- Certificate Owner Notification of an Event
- Private Key Recovery (Key Escrow)
- Certificate Archival and Retrieval Following Expiration

In order to test the digital signature and encryption aspects of the certificates, the first ten certificates were assigned to one writer and the second ten were assigned to the other. Table 4 lists the certificates, their assigned user and the aspect of the life-cycle they were used to test. There is duplication in the tests to ensure that the certificates work for multiple users and that each aspect works consistently. Keep in mind that aspects of the certificate life-cycle including certificate request and certificate download by owner were tested for each certificate simply by creating the certificate. They are not listed for

individual test, because without successful implementation, they rest of the test could not be performed. Private Key Recovery and Key Escrow (Archival) are not assigned to specific certificates because of configuration issues. This is discussed in the adjustments section at the end of this chapter.

Certificate	Test Type	Email Address
Test1	Normal expiration	User1
Test2	Normal expiration	User1
Test3	revocation for cause	User1
Test4	revocation for cause	User1
Test5	revocation by user	User1
Test6	revocation by user	User1
Test7	renewal notification	User1
Test8	renewal notification	User1
Test9	revocation for cause	User1
Test10	revocation for cause	User1
Test11	Normal expiration	User2
Test12	Normal expiration	User2
Test13	revocation for cause	User2
Test14	revocation for cause	User2
Test15	revocation by user	User2
Test16	revocation by user	User2
Test17	renewal notification	User2
Test18	renewal notification	User2
Test19	revocation for cause	User2
Test20	revocation for cause	User2

Table 4. Test Certificate Use and User

B. CONDUCTING THE TESTS

1. Certificate Request, Request Approval and Import

Both users requested certificates for each of their 10 certificates via the RA's SSL end-entity webpage at https://cdntest.cs.nps.navy.mil:1037/ (Figure 25). For testing

purposes, one certificate was used both for the digital signature and digital encryption, also known as a dual use certificate[48], and was created by selecting the **Manual User Dual Use Certificate Enrollment** form.

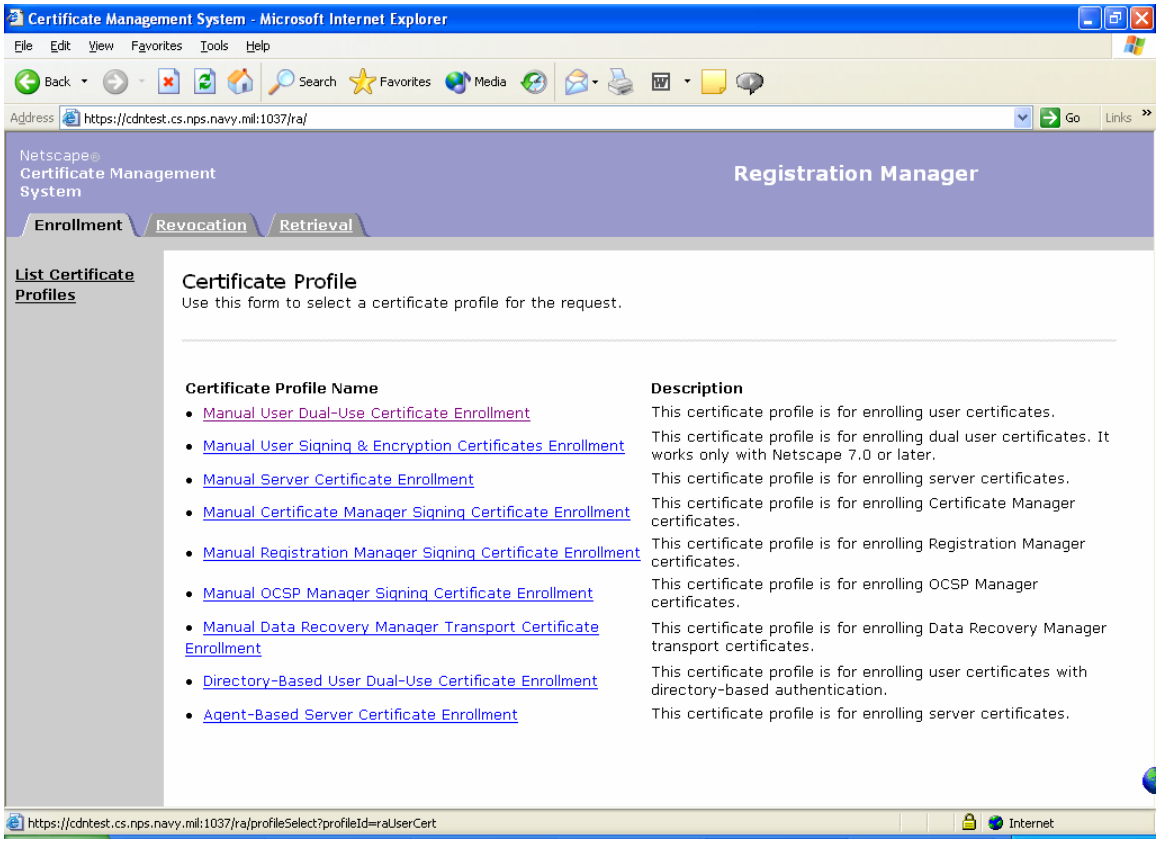


Figure 25. SSL End-Entity Page of RA.

Once the certificate request has been made, it is received by the RA and approved by the RA agent. The request is then signed using the RA signing certificate and sent to the CA. If the request matches an established profile and the certificate matches the one associated with the RA user, a certificate is issued and an email is sent to the owner indicating as such. With a compressed time schedule, the RA agent modifies the validity period of the certificates depending on the purpose of the test. The default time is close to seven months and can be no longer than 365 days. The request, as seen by the RA, is shown in Figure 26. The approval of the certificate request triggers an email sent by the CA to the owner's email address notifying them of the certificate creation. Once this

[48] X.509.

email is received the owner can import her certificate into her browser. This is done by clicking on the retrieval tab of the RA's end-entity interface and entering the appropriate request number. Other people's certificates can also be manually downloaded by users via the CA's end-entity page. Using the **List Certificates** link of the Retrieval tab, they can then copy the base 64 encoding of the certificate to a text file, save it as a .p12 file and then import that .p12 file into their browser. All of the certificates were successfully created, imported into the owner's browser and downloaded by a user.

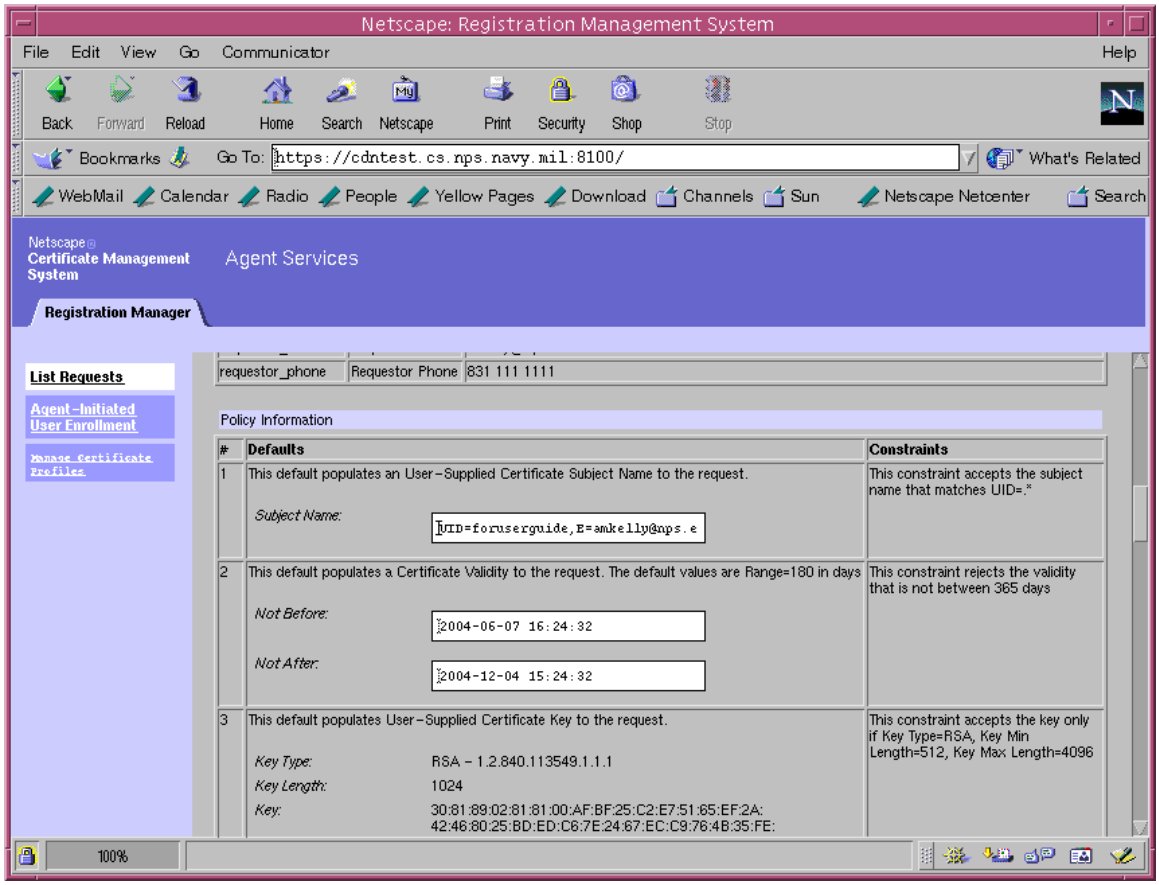


Figure 26. Certificate Request as Viewed from the RA's Agent Interface.

2. Digital Signature and Encryption Testing

Once the certificates have been imported into the Internet Explorer (IE) browser, they can be used by Microsoft Outlook for digitally signing and encrypting email. For each of the 20 certificates, two emails were sent to confirm that the certificates worked for those purposes and were accepted as valid. Figure 27 shows the message security

properties for one of these test emails. As shown, the certificate is not valid for either digital signing or encryption. There is a disconnect in the logic of Microsoft and CMS for CRL checking, so a hard wired solution was used.

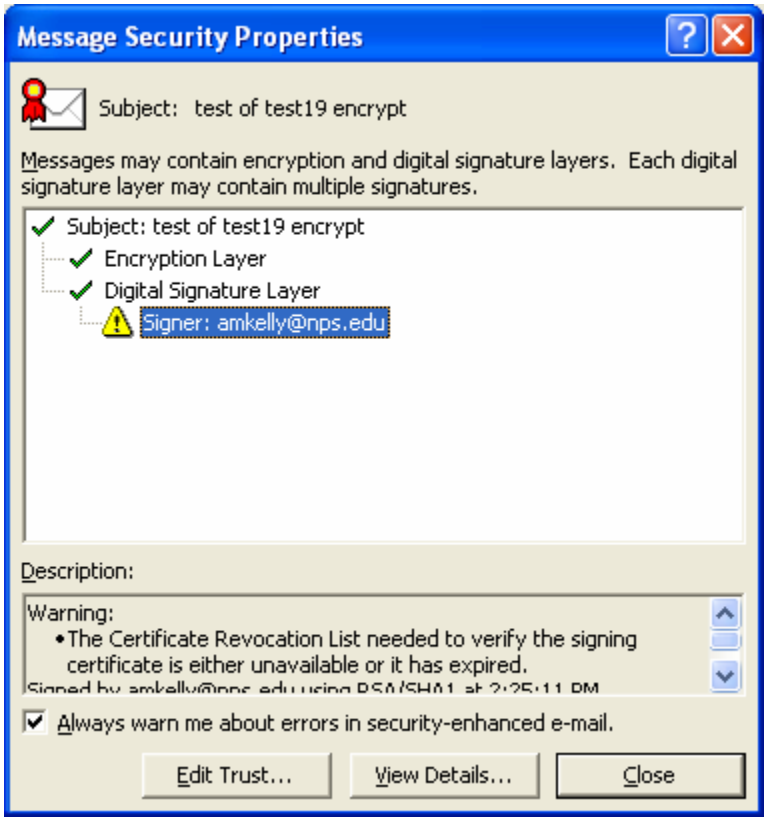


Figure 27. Message Security Properties without a Valid CRL.

a. Manually Importing a CRL

Outlook was unable to verify the validity of the certificates because its locally cached CRL had expired, and it was unable to use the OCSP service provided by the CA. As an alternative revocation check solution, the user can manually retrieve and inspect the CRL maintained by the CA. To manually retrieve a CRL, the user would go to the CA's end-entity page and click on the retrieval tab. On the left side, the user would select **Import Certificate Revocation List**. Next, select the radio button next to **Import the latest CRL** to your browser and click **Submit** (Figure 28).

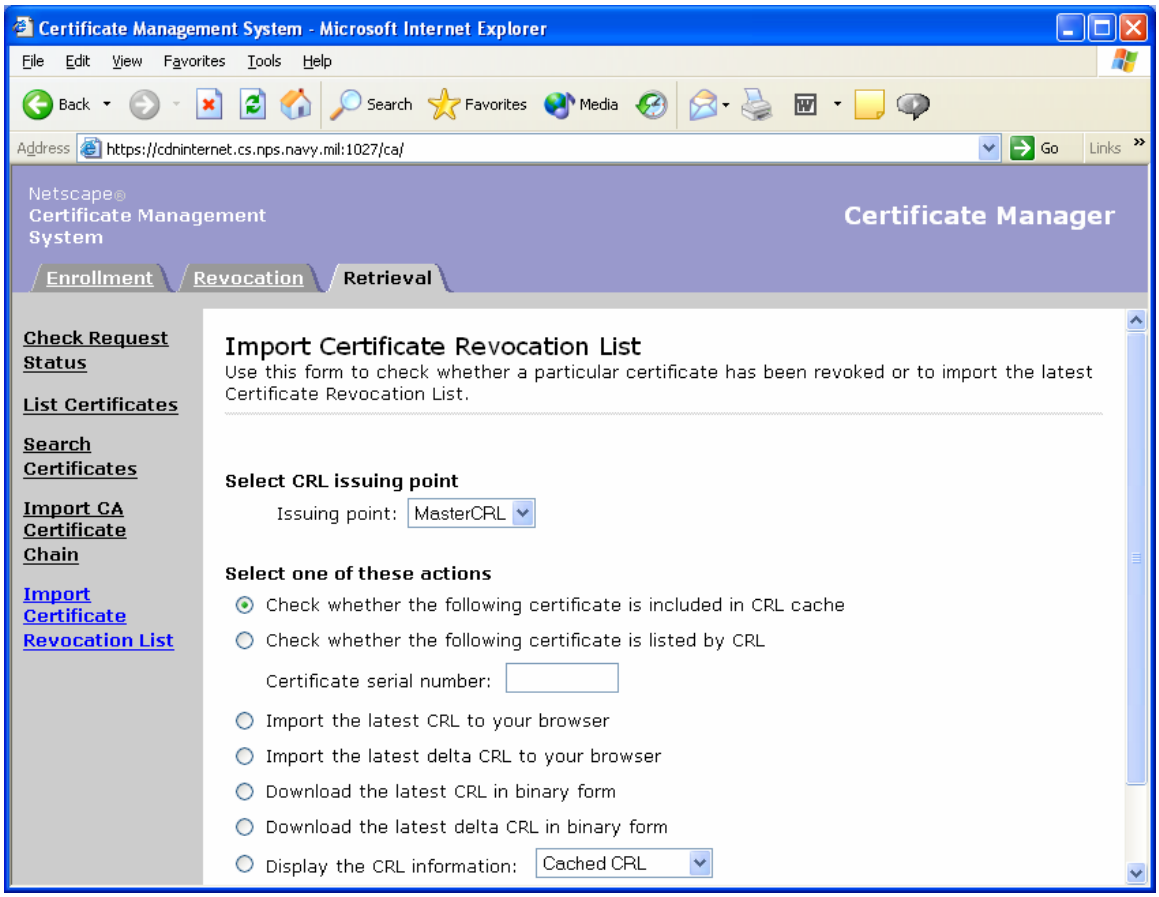


Figure 28. CA End-Entity Page

In IE, the result is a box with the choice to open the file or save it to disk. Once the file is saved the user would right-click on it and select install CRL and follow the steps of the Certificate Import Wizard. Upon completion of these steps, the Message Security Properties showed that the certificate was valid (Figure 29).

Figure 29. Successful verification of certificate after a manual import of the CRL.

All 20 certificates were successfully verified for their validity and use for digital signatures and encryption.

3. Certificate Expiration and Renewal

Eight of the certificates were used to verify that certificates would expire at the end of their validity period that the certificate owner would receive an email reminding them to renew their certificate, and that a certificate could successfully be renewed.

a. Renewal Notification

The CA configures the job scheduler to send out renewal notifications to the owner of certificates at given points in the certificates life-cycle. For the purposes here, certificate renewals were sent out three days before and after a certificate's expiration date. The email includes the expiration date, information from the certificate, and a link where the certificate can be renewed. One such email is pictured in Figure 30. The CA can also be configured to send a renewal notification summary to an agent of the CA. All of the certificate renewal notices and summaries were received correctly.

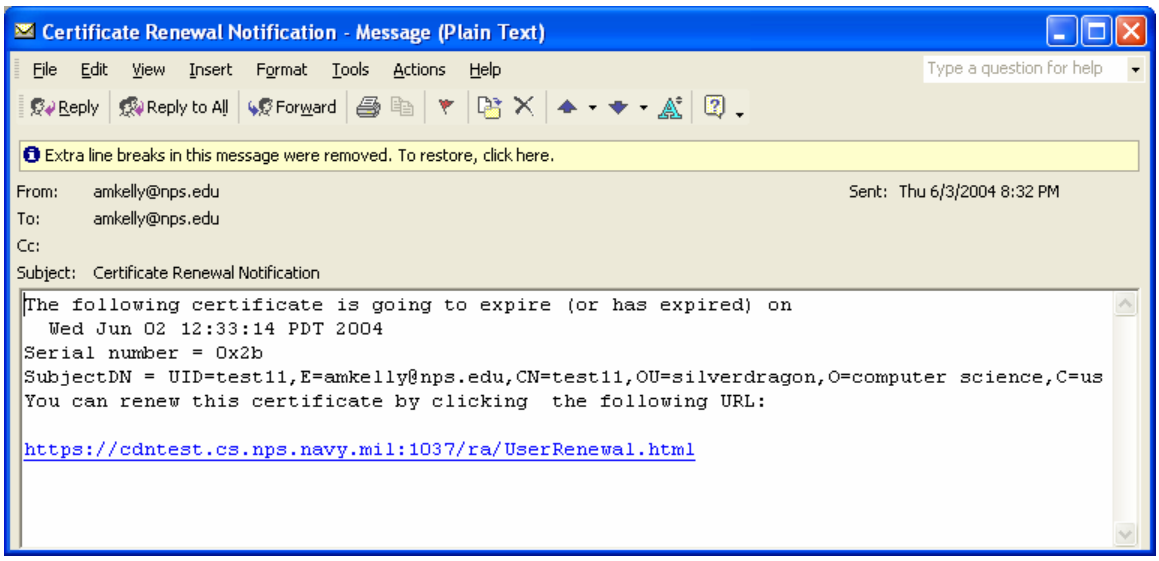


Figure 30. Certificate Renewal Notification Email

b. Verification of Expiration

Once four of the certificates had expired, the emails sent using those certificates were checked to see if the system still recognized them as valid certificates (Figure 31). Successfully, all were considered invalid because they had expired.

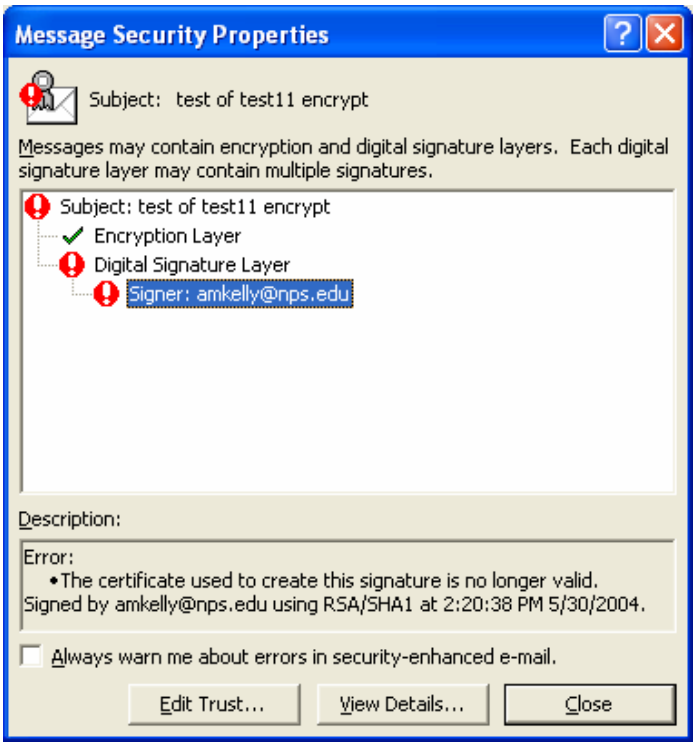


Figure 31. Verification of Certificate Expiration.

c. Certificate Archival and Retrieval Following Expiration

During the certificate approval process, issued certificates are saved in the Directory Server of the CA. Certificates will be kept until a time configured by the administrator or until manually deleted by an administrator. All 20 certificates were successfully archived in the Directory Server. Certificates that have expired can be recovered via the agent interface of the CA using the **List Certificates** link. Once the agent has navigated to the certificate, they can then copy the base 64 encoding into a .p12 file and import it into a browser as needed. All certificates are archived in the Directory Server until otherwise deleted based on a time limit or manually deleted.

d. Certificate Renewal

As mentioned before, once a certificate comes within a specific time range of its expiration date, email notifications are sent out reminding the owner to renew the certificate. By following the link in the email, the owner can then renew their certificate. To renew the certificate, they simply click submit (Figure 32) and then select the certificate they wish to renew from the list that pops up. The resulting certificate request is forwarded to the CA via the RA and a new certificate, valid starting at the date the old certificate expires, is created by the CA and imported into the browser. All four attempts at certificate renewal were successful and verified by sending new emails (digitally signed and encrypted) using the renewed certificates.

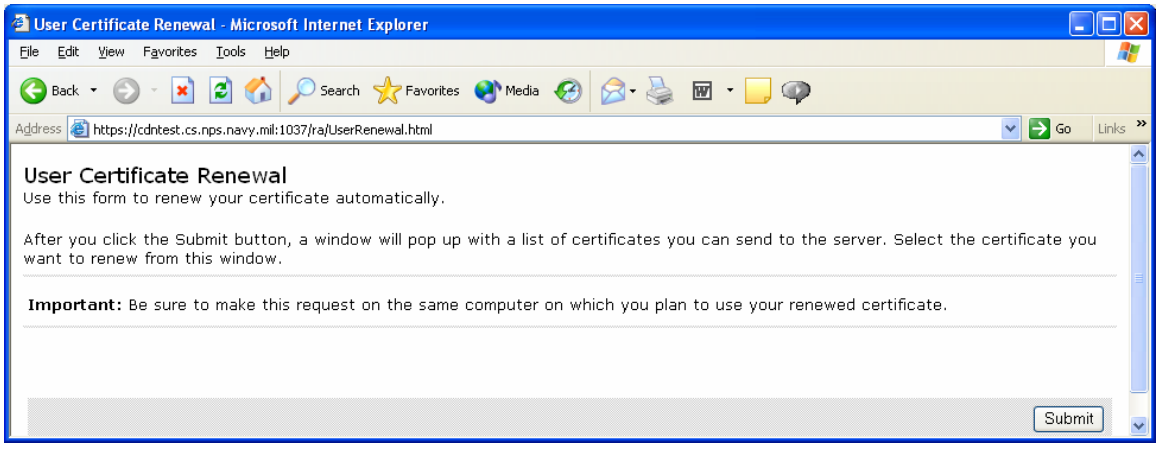


Figure 32. User Certificate Renewal End-Entity Page

4. Certificate Revocation

A key factor in the effectiveness of a PKI system is to be able to revoke certificates whose corresponding private keys have been compromised, or whose owners have been either transferred from an organization or otherwise lost certain privileges that were validated by the certificate. In the CMS, there are two methods of revocation, user and agent.

a. Revocation by User

If a user (or owner) determines that his certificate has been compromised in some form, he can revoke his own certificate. This is done by going to the secure end-entity interface of either the RA or CA and clicking on the revocation tab (Figure 33). The user will then specify the reason for revocation and the specific certificate to be revoked. The CA or RA will process the request and the revoked certificate will show up on the next CRL. In our tests, all of the user revocations were successful. This was checked by entering the serial numbers of the certificates at the **Import CRL Revocation List** link to verify that the certificates were on the revocation list. Unfortunately due to configuration problems with Microsoft products, verification that a certificate had been revoked via the browsers certificate store or via Outlook for failed.

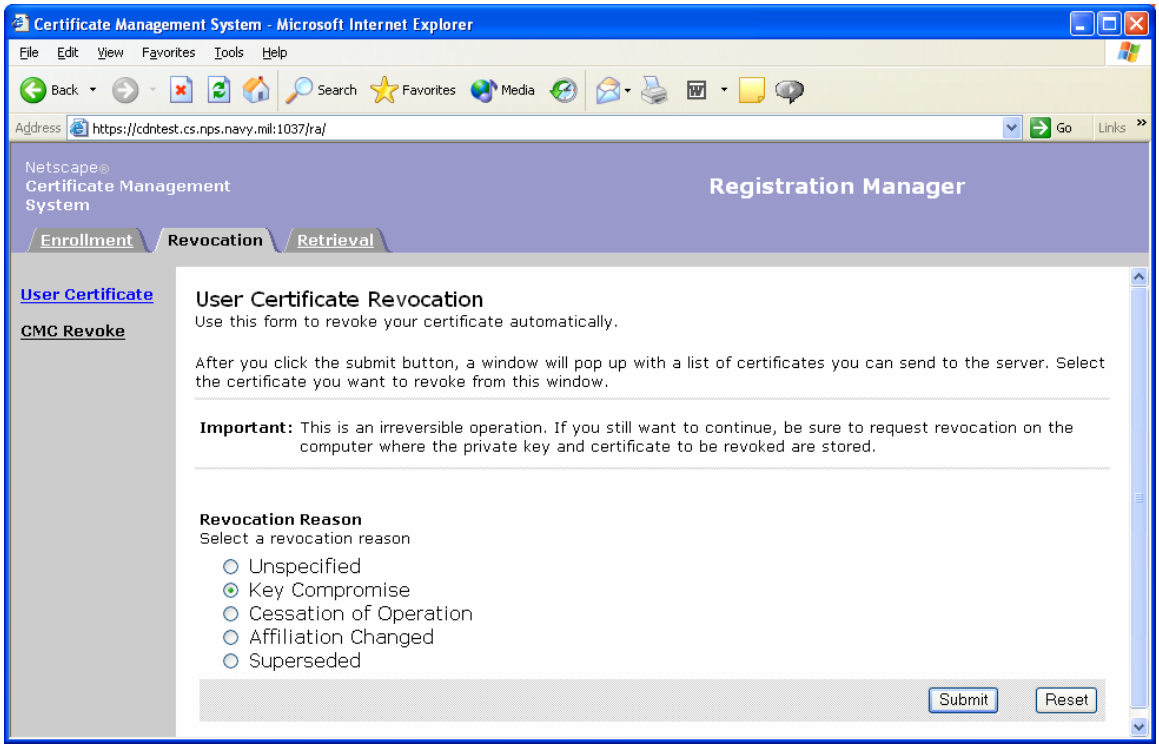


Figure 33. User Certificate Revocation Form

b. Revocation for Cause

A CMS agent can revoke a certificate at any time for any reason. If an employee is fired, an administrator may wish to terminate their certificate at the earliest time to prevent potential loss of data or proprietary information belonging to the company. This can be done using the agent interface of the CA. The agent is given the same reasons for revocation as the user is, along with the additional option of "CA key compromised". Once the certificate has been revoked it will show up on the next CRL. The test of eight certificates for revocation for cause were successful and verified using the CA's end-entity interface as was done for testing revocation by user (above).

c. Revocation Issues

As mentioned in the previous two sections, there is an issue with CRL checking. First, to enable CRL checking in IE and Outlook some configuration changes need to be made. In the advanced security setting of Internet Options in IE, both "check for publisher's certificate revocation" and "check for server certificate revocation" need to be checked. For Outlook, a registry key must be added to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\ with the name

{7801EBD0-CF4B-11D0-851F-0060979387EA}. The next step is to create the DWORD registry value PolicyFlags and set to the hexadecimal value of 10000.[49] In addition to these changes, the CA must be considered a Trusted Root CA by the operating system. Although these changes were made, there is still a mis-configuration issue that hinders proper CRL-based revocation checking. As discussed in the Adjustments section later in this chapter, the CRL Distribution Point Extension that was not included in the certificates for these tests may help with this issue.

C. SUMMARY OF RESULTS

Table 5 is a summary of the certificates, the tests they were used for and the results. All of the tests were successful. The cells that are blacked-out are not applicable to the test in that column. For example a certificate that was used to test revocation was not used to test renewal after that.

Username	Test type	certificate download by owner	certificate download by user	normal expiration	revoked	revocation notice received	usage for digital signing	usage for encryption	renewal notification received	renewed
test1	normal expiration	Yes	yes	Yes			yes	yes	yes	yes
test2	normal expiration	Yes	yes	Yes			yes	yes	yes	Yes
test3	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test4	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test5	revocation by user	Yes	yes		yes	yes	yes	yes	yes	
test6	revocation by user	Yes	yes		yes	yes	yes	yes	yes	
test7	Renewal notification	Yes	yes	Yes			yes	yes	yes	yes
test8	Renewal notification	Yes	yes	Yes			yes	yes	yes	yes
test9	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test10	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test11	normal expiration	Yes	yes	Yes			yes	yes	yes	yes

[49] Interview via email between V. Beach, SPAWAR Systems Center and authors, June 14, 2004.

Username	Test type	certificate download by owner	certificate download by user	normal expiration	revoked	revocation notice received	usage for digital signing	usage for encryption	renewal notification received	renewed
test12	normal expiration	Yes	yes	Yes			yes	yes	yes	yes
test13	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test14	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test15	revocation by user	Yes	yes		yes	yes	yes	yes	yes	
test16	revocation by user	Yes	yes		yes	yes	yes	yes	yes	
test17	Renewal notification	Yes	yes	Yes			yes	yes	yes	yes
test18	Renewal notification	Yes	yes	Yes			yes	yes	yes	yes
test19	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	
test20	revocation for cause	Yes	yes		yes	yes	yes	yes	yes	

Table 5. Summary of Certificate Tests Results

D. ADJUSTMENTS

Though all of the tests were successful, there are a few areas that can be streamlined. The first issue is the CRL checking. For the purposes of these tests, CRLs had to be manually installed into Windows. The ultimate goal for revocation checking would be to have a CRL Distribution Point Extension in the certificate that used ldap to reach the CRL published to the CRL Issuing Point in the Directory Server. This extension should also be added to the CA signing certificate. It is not known where the problem exists, whether it is a Microsoft implementation issue, a Netscape implementation issue, an X.509 PKI design or configuration issue, or some combination of these.

Key archival and recovery is an area that was not tested due to a configuration issue. Based on the log files of the CA, RA, and DRM there appears to be no archival request being sent to the DRM during the certificate request and approval process. The

correct certificate for the DRM Transport Certificate is being used to transport the private key and this can be verified when the user is prompted that the CA wishes to archive the owner's private key. It appears that there is a trust issue between the CA and the DRM that prevents the key archival request from being processed. As discussed in Chapter 4, the goal of key archival is to store the private key of the certificate owner during the certificate request and creation process. Recovery would then include retrieving the private key and its corresponding certificate in case it was deleted from the user's machine or to open documents once a user has left his/her organization. In the DRM, key recovery is performed by recovery agents, via the DRM's agent interface, using passwords to unlock the DRM storage key, retrieve the decrypted private key, and create a PKCS #12 package that includes the private key and its corresponding certificate. In the CISR PKI lab, there is a trust relationship problem that prevents the storage and retrieval of private keys. Once the communication between the CA, the RA, and the DRM is configured correctly, this process can be tested properly.

VI. CONCLUSIONS

A. OBSERVATIONS

The greatest observation of PKI that can be offered at the conclusion of this thesis is that implementing a PKI is not trivial. For an administrator to fully comprehend and manipulate the capabilities of Netscape's CMS, they must understand Solaris, PKI fundamentals and standards, HTML, Java, JavaScript, LDAP directory structure, and LDAP communications. That being said, instituting a CA test facility at NPS will allow for further research in Public Key Infrastructure and thereby, assist DoD in achieving its goal of department-wide use of PKI and Public Key Enabled (PKE) services. This thesis consisted of implementing a prototype Certificate Authority and it supporting infrastructure. In it, PKI was defined, a brief history of public key cryptography was provided, and certificate usage was reviewed. This was followed by a discussion of the various policy considerations. A descriptive overview of the installation was provided with the ensuing tests well documented. The road to establishing a public key infrastructure has been filled with many unexpected turns and a few pitfalls, the next section will discuss some of the issues encountered.

B. ISSUES

Software and hardware selection was the easy part in that the Sun Blade 100's were available and DISA provided access to the Netscape CMS software. The configuration and integration of the hardware and software became the major challenge. The first problems were encountered during the installation of the CMS software. The final installation was reached after reformatting and partitioning the hard drives, memory upgrades, and close to twenty CMS installation attempts using different deployment schemes and configurations. These problems can be attributed to several factors:

- A lack of DoD documentation on how to build a PKI
- A lack of Netscape documentation on how to build and implement their PKI
- The learning curve required to understand the Solaris operating system, PKI fundamentals and the components used to build the CMS software.

Progression through the installation helped to provide a foundation in the understanding of the CMS, however more help was required for the implementation of certificate

profiles, CRL publishing, and certificate extensions. Fortunately, expert technical assistance was obtained from Code 2873 at SPAWAR Systems Center San Diego provided a large knowledge base on PKI and CMS.

With the knowledge acquired from SPAWAR and the installation complete, it was time to move onto the configuration of the PKI. Trust relationships between the CA, the RA, and the DRM were established. Certificate profiles were adjusted to allow users to request certificates via the RA and to allow owners' private keys to be archived. The MasterCRL was enabled and configured to provide access to a CRL issuing point and LDAP publishing of this CRL was also enabled. Though the majority of the operational functionality of the PKI was established and the certificate life-cycle tested, there are two areas that remain for follow on research before this PKI is fully functional.

C. FOLLOW ON WORK

During the testing of the PKI operations there were two areas that were identified as requiring further work. Certificate validation is the first concern. Microsoft products must be manually configured to perform CRL checking as discussed in Chapter 5. One way to facilitate this process is to include the Certificate Revocation List Distribution Point certificate extension in the certificates. This extension must be included in the CA signing certificate as well as user certificates. The extension points to the location of the CRL in the Directory Server and this CRL issuing point must be readable by all users to allow for the revocation checks to occur. Correct implementation of this extension and CRL publishing will streamline the CRL checking issues and make the PKI more effective for future research.

The second operability issue is the escrow and recovery of private keys, what CMS refers to as "key archival." Key archival is the process through which private keys are stored in the DRM during the certificate request and approval process. As discussed in Chapter 4, private keys are encrypted using the DRM's storage certificate and then stored in the DRM's Directory Server. The current configuration requires two recovery agents (of a possible four) to enter their passwords to unlock the storage encryption. A PKCS #12 package containing the private key and its associated certificate is then created. Currently, a trust issue prevents the key archival request created by the certificate request from being processed. With no keys archived, key recovery cannot be

tested. Reissuing the certificates for the CMS subsystems using the Certificate Setup Wizard and making the necessary configuration adjustments may fix the problem. This functionality is important for any environment that deems private key recovery an essential aspect of its PKI.

The ultimate goal of this project was to create a PKI test bed in the NPS CISR lab that would enable testing of current DoD PKI issues. Ideally, with the two problems described above fixed, other areas of PKI research including validation, verification, CRL distribution, and Online Certificate Status Protocol (OCSP) can be performed, thus improving the DoD's ability to secure communications in a computer network environment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

This appendix is the User's Guide to the CISR PKI. It outlines installation procedures and provides step by step instructions for the performance of software configuration and maintenance. The User's Guide is intended for use in follow on research or by students during cyber defense exercises.

PUBLIC KEY INFRASTRUCTURE

NPS CISR Lab

User's Manual

NAVAL POSTGRADUATE SCHOOL

Public Key Infrastructure User's Guide

LCDR Vanessa Ambers, USN
1LT Amanda Kelly, USAF
June 2004

Table of Contents

Getting Started 4
Familiarization with Solaris 8 4
Solaris References 4
Preparing the Computer 4
Adjusting Network Configuration 4
Creating Groups and Users 6
Extracting CMS Software 7
Installation 8
Installing the Netscape Servers 8
First Server Group Installation 8
Second (Multiple) Server Group Installation 14
Configuring the CSM Instance 16
Connecting the Subsystems 30
User Certificates 34
Certificate Issuance 34
Owner Request 34
Request Approval 36
Owner Retrieval 36
Revocation 38
Owner Revocation 38
Agent Revocation 40
Installing CRL 41
Renewal 44
Importing and Exporting Certificate & Keys 46
Export 46
Import 47
Server Certificates 49
Managing Certificates 49
Certificate Setup Wizard 50
Requesting a New Certificate 50
Installing a New Certificate 53
Users and Groups 54
Users 54
Add 54

Delete 57
Groups 57
Add 57
Delete 58
Notification and Jobs 60
Setting Up the Mail Server 60
Enabling Notifications 61
Job Scheduler & Jobs 62
Certificate Profiles 66
Approve or Disable a Profile 66
Adding a Certificate Profile 66
Editing a Certificate Profile 70
Deleting a Profile 71
Publishing and CRL Issuing Points 72
Configuring the CRL Issuing Point 72
Publishing 75
Key Archival and Recovery 78
Key Archival 78
Key Recovery Scheme 79
Scheme Management 79
Changing Recovery Agent Passwords 81
Key Recovery 82

Chapter 1

Getting Started

Preparing your system for installation Netscape's Certificate Management System.

The installation and configuration of Netscape's Certificate Management System (CMS) requires some preparation of both the user and computer(s) on which the system will be installed.

Familiarization with Solaris 8

Netscape's CMS 6.1 currently runs on Solaris 8. A working knowledge of this operating system is important. A good knowledge of UNIX is beneficial, however there are some differences between Solaris and UNIX commands and system information. The list of references below can help to increase your knowledge of Solaris.

Solaris References

- Solaris Solutions for Systems Administrators 2nd Edition by Sandra Henry-Stocker and Evan R. Marks
- Sun Systems website – www.sun.com/documentation

NPS also boasts several Solaris experts including Mike Williams and Paul Clark. They have experience with Sun systems and can provide some technical support and if nothing else can point you in the right direction to find a solution to a problem.

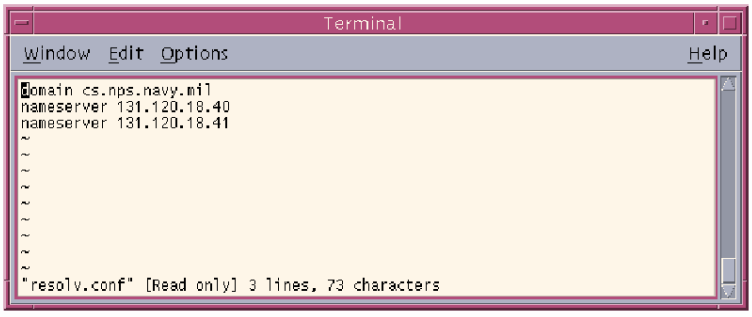
Preparing the Computer

Adjusting Network Configuration

Our recommendation is to begin with a clean installation of Solaris 8, especially if the computer has been inherited from another project. After installing the operating system, there are a couple of files that need to be created or modified to setup DNS

capabilities and the remainder of the networking parameters, if they were not done successfully during the Solaris Installation. The network parameters used below are from a test setup. The network the PKI is being installed on will determine the default router and DNS server(s) used.

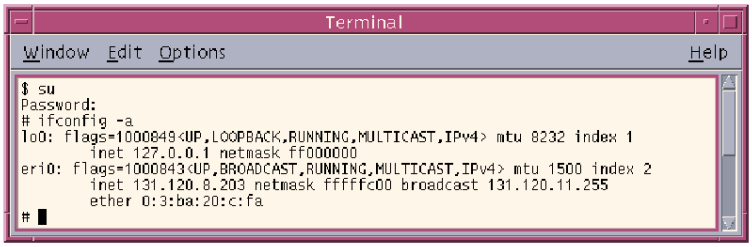
1. Login or su to root and open a terminal window.
2. Change directories to /etc
3. Add the defaultdomain file. This file tells the computer which domain it is associated with and is needed for CMS installation.
    a. vi defualtdomain
    b. Add the line "cs.nps.navy.mil"
    c. Save and close the file
4. Add the defualtrouter file. This file tells the computer the IP address of the router, which it communicates with.
    a. vi defaultrouter
    b. Add the line "131.120.8.1"
    c. Save and close the file
5. Modify or create the resolv.conf file. This file contains the addresses of the DNS servers that the computer can resolve its name and IP address. This is another key file for CMS. If preferred you can setup a DNS server on the computer you are using, although this is not recommended mainly because it is a complicated process. The resolv.conf file should look as follows:



6. Ensure that your IP address and subnet mask are correct.

a. List the current configuration of the NIC.

i. ifconfig –a



b. Modify the address or subnet mask as needed

i. ifconfig eri0 inet 131.120.8.203

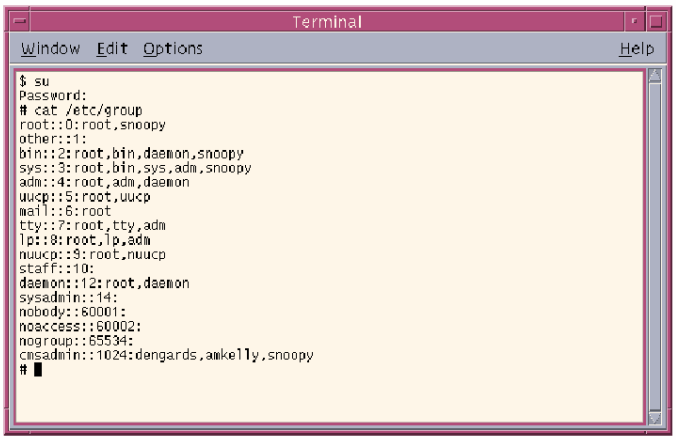
1. eri0 is the name of the NIC card

ii. ifconfig eri0 netmask 255.255.252.0

Creating Groups and Users

Once the network configuration has been setup, groups and users that will be associated with running CMS need to be created. This group will have access to the consoles and files that run CMS. CMS can also run as one of these users depending on your setup. It is suggested that you have a group with a user to run CMS as and another user that will manage the CMS installation.

1. As root, change directory to /etc
2. Open the group file in vi or another editor
3. At the end of the file add the new group name, a number that will serve as the group identifier and any users that will belong to that group. In the picture below, the cmsadmin group has been added with a group id of 1024 and the users: dengards, amkelly, and snoopy.



4. Create the user, profile and set the password. This should be repeated for all of the users that were added.

    a. useradd -g cmsadmin -m -s /sbin/sh -d /export/home/**username** **username**

    b. cp /etc/skel/local.profile /export/home/**username**/.profile

    c. passwd **username**

Extracting CMS Software

The DoD is currently using CMS version 6.1 on all of its Certificate Authorities (CA). This is the version referred to for the duration of this user's manual. The software can be found at the DoD Site License – Netscape Software Download Site at http://netscape.intelligent.net/redisa/. The user must register and sign on to be able to use the site and perform downloads. There is also a cdrom containing the software in the CISR. There are a couple of options for getting the software onto the Sun box. Assuming, the network connection is functional, the software can be downloaded directly to the computer. If there is no connection to the outside world, use a cdrom or ftp the file from a computer with outside access to the Sun box.

1. Copy the cms61.tar file to /export/home/ or another directory

2. Extract the files – tar xvf vms61.tar

The computer is now ready to install the CMS software.

Chapter 2

Installation

Installing the Certificate Management System and CMS Instance Configuration

Installing Netscape's Certificate Management System (CMS) is fairly simple once you decide what your deployment scheme will be. Though you can have multiple CMS instances in one server group, our recommendation is to install multiple server groups and connect via the Directory Server. The CISR lab is setup with a Registration Manager in a server group on Tefnut and a Certificate Manager and a Data Recovery Manager in individual server groups on Maat.

CMS is installed with an administration server instance, a directory server instance and a certificate management server instance. The administration server runs the console used to manage the servers and the directory server keeps track of certificates, requests, CRLS, and user information. The CMS instance will be configured depending on the subsystem you are running and contains the agent, end-entity, and administration web-pages, along with the policies and profiles associated with them.

Installing the Netscape Servers

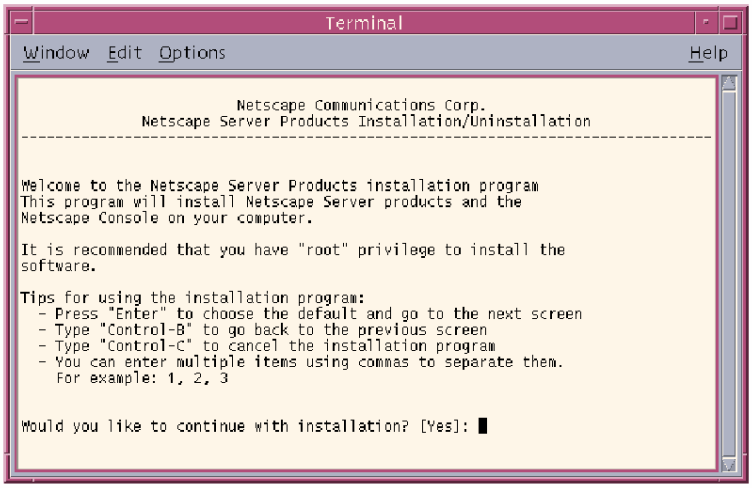
The installation begins by installing the software for the administration server, directory server and the certificate management system. This portion is split into two sections, one if you are installing the first server group on a machine and a second if you are installing another server group on a machine which already has a server group. Multiple instances of the directory server and CMS can be run in one server group. The choice for multiple servers or multiple CMS instances in one server group depends on the deployment scheme. Further explanations of the screens, questions, and configuration information asked for during this phase of the installation are located in the *Administrator's Guide Netscape Certificate Management System, Version 6.1.*

First Server Group Installation

1. Open a terminal window and change directories to the directory you extracted the CMS installation files to.

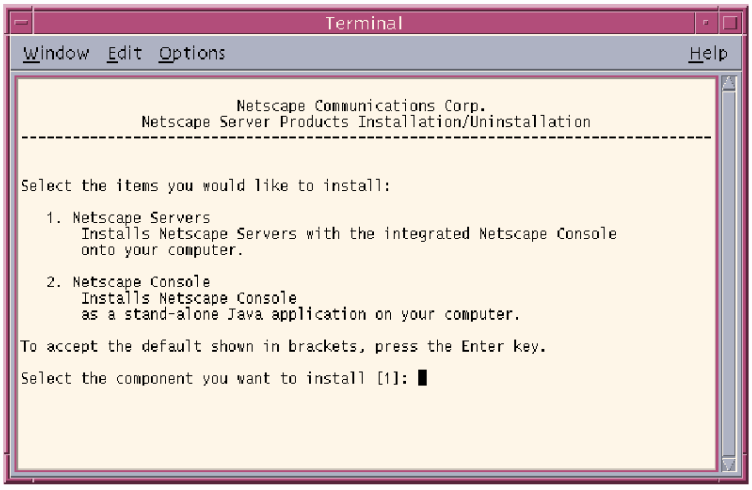
2. Type: ./setup –k (this flag keeps a setup log file that you can read later)

3. Answer yes to continue the installation.



4. Answer yes to accept the license agreement.

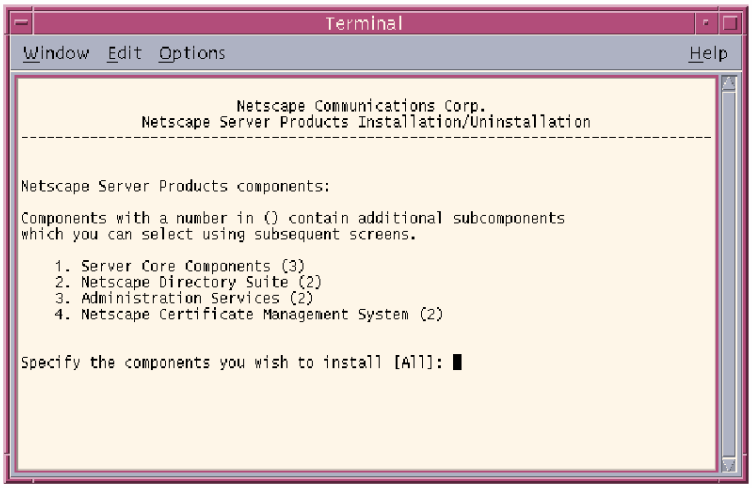
5. Select 1



6. Select 2 – Typical Install

7. Accept the default location or choose a different location

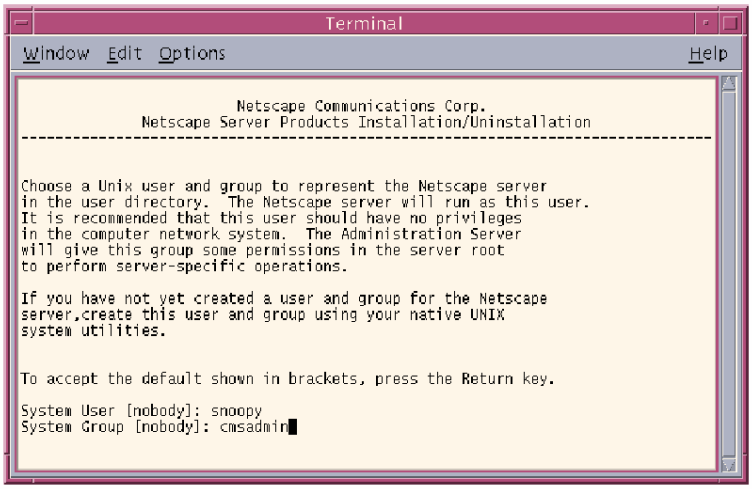
8. Select the defaults for the next six screens about which Netscape servers and their components to install.



9. Enter the fully qualified domain name for the computer.

10. Enter system user that the servers will run as.

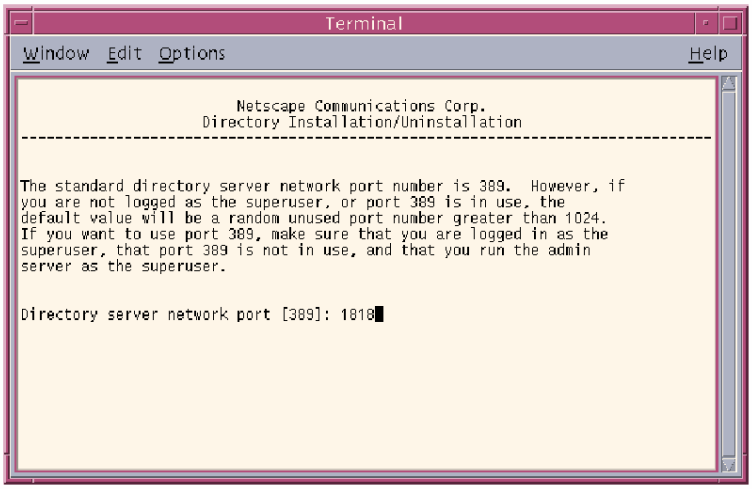
11. Enter system group that the system user belongs to.



12. No, you do not want to register with an existing directory server.

13. No, you do not want to use another directory to store your data.

14. Select the port number that the directory server instance will use. The default is given as 389 which is a standard ldap port. For security purposes, this port should be changed to greater than 1024 so that the directory server can run as your system user id instead of root. If you choose to run directory server as root, the port selected must be 389.



15. Enter an identifier for the directory server, typically the computer name, but it can be anything.

16. Enter the administrator id and password that will be used to log into the administration sever via the console to control the servers.

17. Accept the defaults for the Directory Manager Distinguished Name.

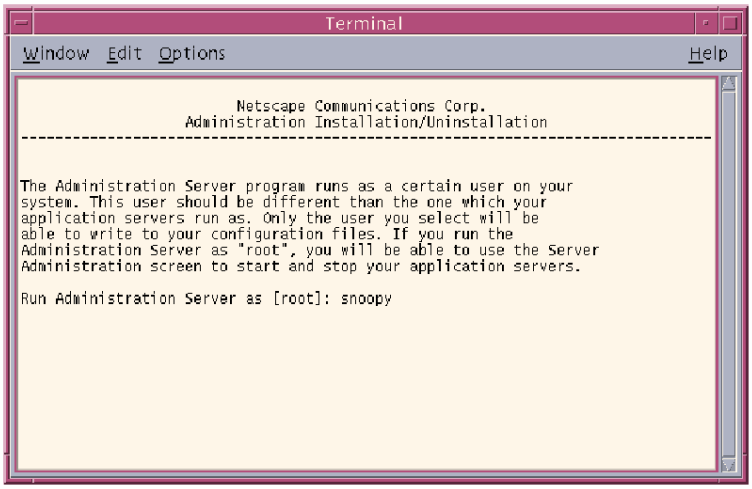
18. Select the default domain name for the directory manager.

19. Enter the password of the system user.

20. Enter the administration domain. The correct portion of the fully qualified domain name should come up as the default.

21. Enter the administration port number. This number should be above 1024 and the default is acceptable.

22. For security purposes, run the administration server as the system user id.



23. Enter the identifier for the CMS instance in the server group.

You should get the following output and then you are ready to proceed to the configuration of the CMS instance or a second server group installation.

Second (Multiple) Server Group Installation

1. Open a terminal window and change directories to the directory you extracted the CMS installation files to.
2. Type: ./setup –k (this flag keeps a setup log file that you can read later)
3. Answer yes to continue the installation.
4. Answer yes to accept the license agreement.

5. Select 1
6. Select 3 – Custom Install
7. Accept the default location or choose a different location
8. Select the defaults for the next six screens about which Netscape servers and their components to install.
9. Enter the fully qualified domain name for the computer.
10. Enter system user that the servers will run as.
11. Enter system group that the system user belongs to.
12. Yes, you do want to register with an existing directory server.
13. Enter the fully qualified domain name and port number of the directory server of the first server installation.
14. Enter the admin id and password for the directory server you are connecting to.
15. Select the port number that the directory server instance will use. The default is given as 389 which is a standard ldap port. For security purposes, this port should be changed to greater than 1024 so that the directory server can run as your system user id instead of root. If you choose to run directory server as root, the port selected must be 389.
16. Enter an identifier for the directory server, typically the computer name, but can be anything.
17. Accept the default dns.
18. Select the default domain name for the directory manager.
19. Enter the password of the system user.
20. Choose either yes or no.
21. Choose either suggest or none.
22. Choose no.
23. Enter the administration port number. This number should be above 1024 and the default is acceptable.

24. Enter the IP address of the computer on which you are installing the software or leave blank.

25. Enter the system user id.

26. Enter the identifier for the CMS instance for the second server group.

Configuring the CSM Instance

The CMS instance now needs to be configured for the subsystem you are running on that particular server group or just for that particular instance. CMS has four possible subsystems that it can run as: a certificate manager (CA), a registration manager (RA), a data recovery manager (DRM) (also referred to as a key recovery archive (KRA) in some environments), and an online certificate system manager (OCSM). The CA subsystem also has two possible setups, one for a root CA and one for a subsidiary CA. Each subsystem has a different installation wizard however the first few steps are the same.

1. From a terminal window, change directories to the main server groups directory. Type ./startconsole to start the Netscape console. Enter the user name and password for the administration id used for the administration server during installation.

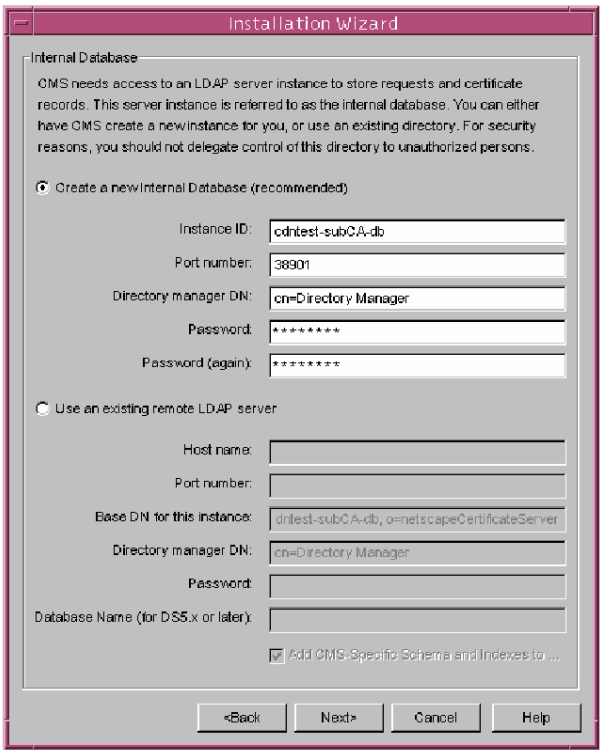
2. Double click on the CMS instance you will be working with.

3. Click next.

4. Enter a logon token.

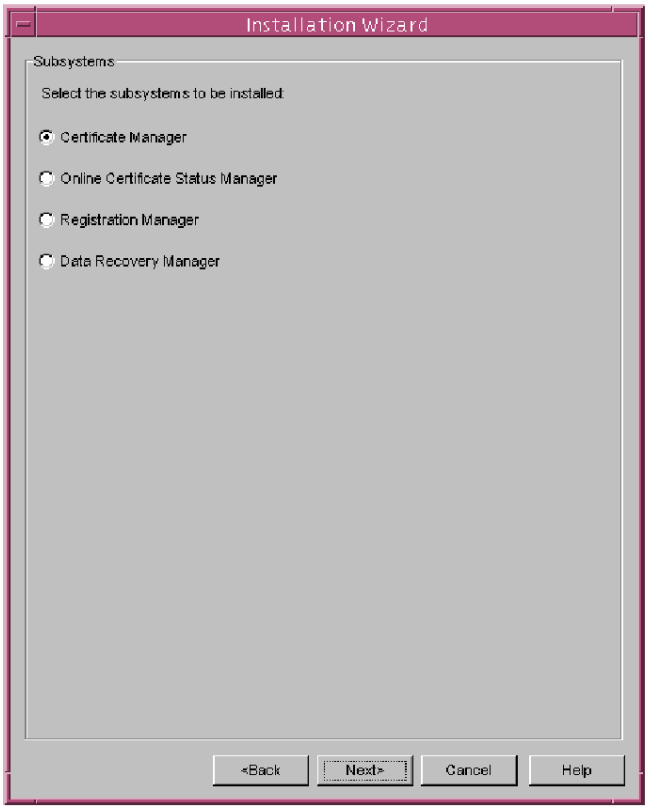
5. The recommendation is to select the default of creating a new internal database. Enter the required information.

    a. Note: If the installation hangs during this process. Halt the system from a terminal window. Restart the slapd server and that administration server. Remove the directory of the internal database, it will have –db after the instance name. Finally, start the console and restart the setup wizard.



6. Administrator Information: Enter the administrator id and password. Leave the allow multiple roles for users checked.

7. Select the subsystem you will be installing.



Certificate Manager

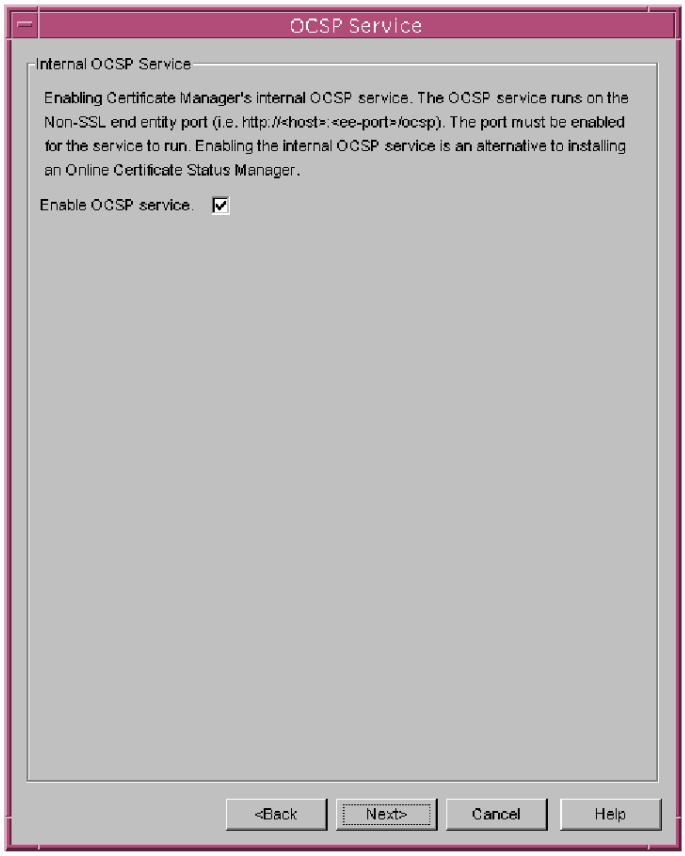
1. Since you have not setup a DRM, answer no to do you want to connect the current subsystems to a remote data recovery manager.

2. Enter the serial number range.

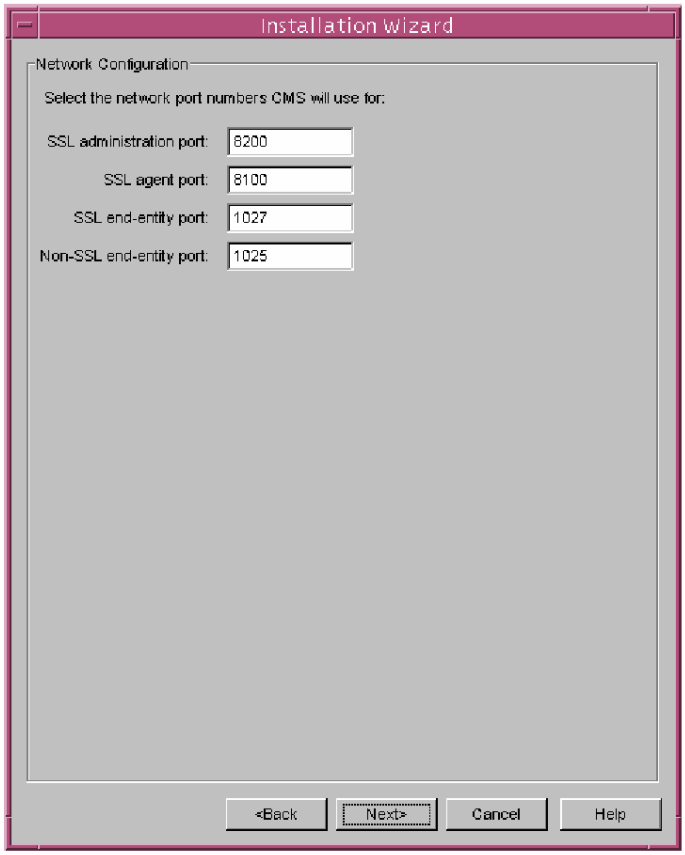
    a. Root CA: The starting serial number should be left at 0x1. If you are not installing a subsidiary CA, you can leave the ending serial number blank. If you are adding a subsidiary CA, our recommendation is to set an upper bound for the Root CA.

b. Subsidiary CA: The starting serial number should be the Root CA's ending serial number plus one. The ending serial number can be left blank or if there are multiple subsidiary CAs an upper bound should be set so that the subsidiary CAs are not issuing numbers in the same range.

3. Leave the internal OCSP service box checked. You can enable and disable this box via the CMS console if you choose to use it later, but if the box is left checked an OCSP certificate will be created during install and the OCSP responder information will be setup.



4. Select the ports that the various services will be running on. As long as they are above 1024 and aren't being used by other daemons, any number will work.



5. For the Root CA select to create a self-signed CA Certificate. If you are installing a subsidiary CA, you will need to follow the instructions for acquiring a certificate located in the both the DRM (#6 – 15) and RA (#23) sections.

6. Enter the Key-Pair Information. If you are using a cryptographic module you can select an external token. The key length can be 1024, 2048 or a custom bit length.

a. Token: Internal

b. Key Type: RSA

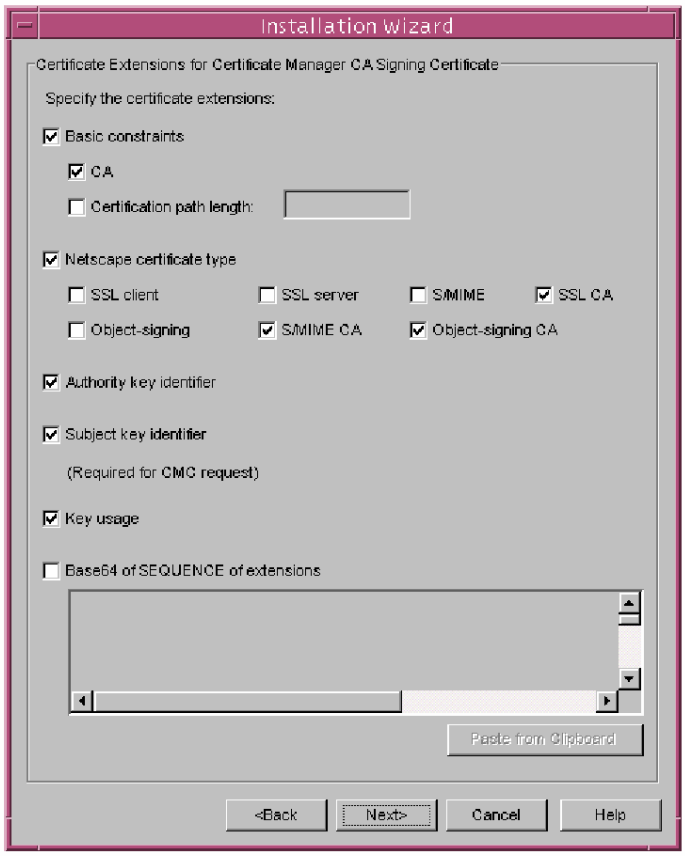
c. Key Length: 2048

7. Select a Message Digest Algorithm: SHA1

8. Enter the Subject Name information for the Certificate Manager CA Signing Certificate. Enter as much or as little information as you want. You should include a common name, the organizational unit, the organization and the country.

9. Modify the Validity Period as needed.

10. Keep the default Certificate Extensions.



11. Click next.
12. Select sign SSL Certificate with my CA Signing Certificate.
13. Modify key-pair information for the SSL Server Certificate as needed. The key length cannot exceed that of the CA Signing Certificate.
14. Select the Message Digest Algorithm.
15. Enter the subject name information for the SSL Server Certificate.

16. Modify the Validity Period. It should not extend past the validity of the CA Signing Certificate.

17. Accept the default certificate extensions.

18. Click next.

19. Check the remove password.conf file. As long as you have maintained records on the passwords you are using, remove this file, since they are stored in the clear for use when starting, stopping and restarting the servers. There is another location where the information is encrypted and saved.

Once you have completed the setup of the root CA, the first agent must be enrolled. Members of the agent group have access to the agent services portion of the CA website and the CMS console. Agents can add and change certificate profiles or policies, issue and revoke certificates and control other aspects of the subsystem. The first agent enrollment is only needed for the CA subsystem. Follow the instructions below to setup the first agent.

1. Open a browser and go to https://host:adminport/ca/adminEnroll.html

2. Fill out the information on the form. Remember that the validity date cannot be past the validity date of the CA signing certificate and the key length cannot be longer than that of the CA's. You will need to enter a password for the key storage used in the browser.

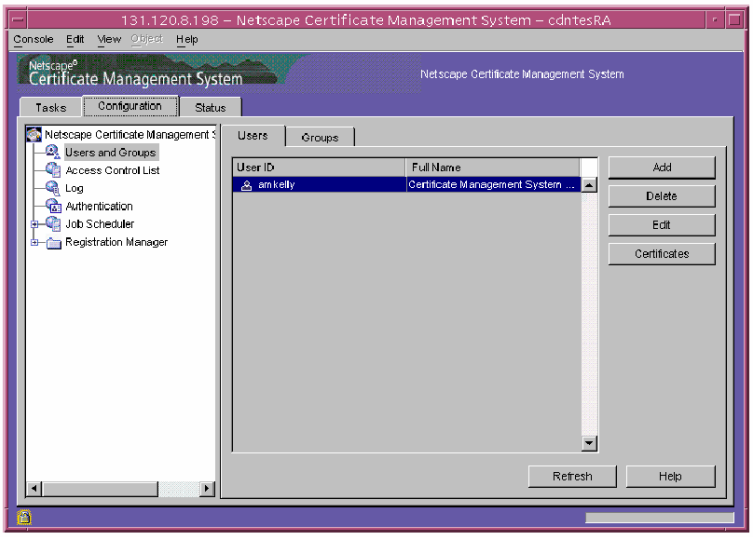
3. The CA will then issue the certificate and you will now have access to the agent. Copy the base 64 encoding of the certificate from the page in the browser.

4. Open the CMS console, by double clicking on the instance in the Netscape Console.

5. Click on the configuration tab.

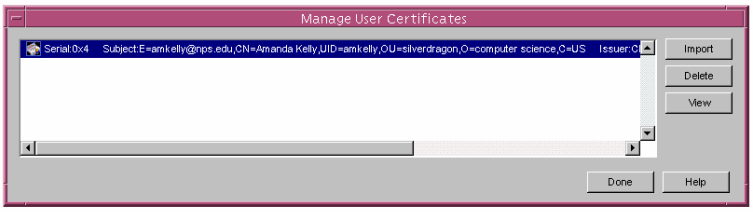
6. Click on Users and Groups.

7. Select the user you entered as the administrator.



8. Click Certificates.

9. Click Import.



10. Click Copy from Clipboard to copy the 64-base encoding from step #3 into the window.

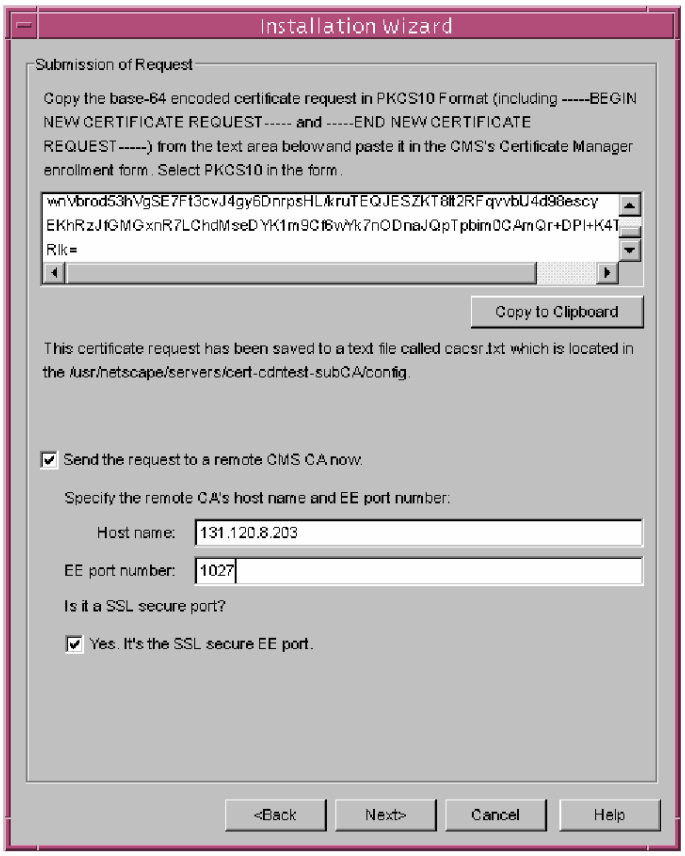
11. Click Done. Note: If the certificate is rejected for some reason, simply repeat the copy and import process.

The Root CA is now ready to be configured.

Data Recovery Manager

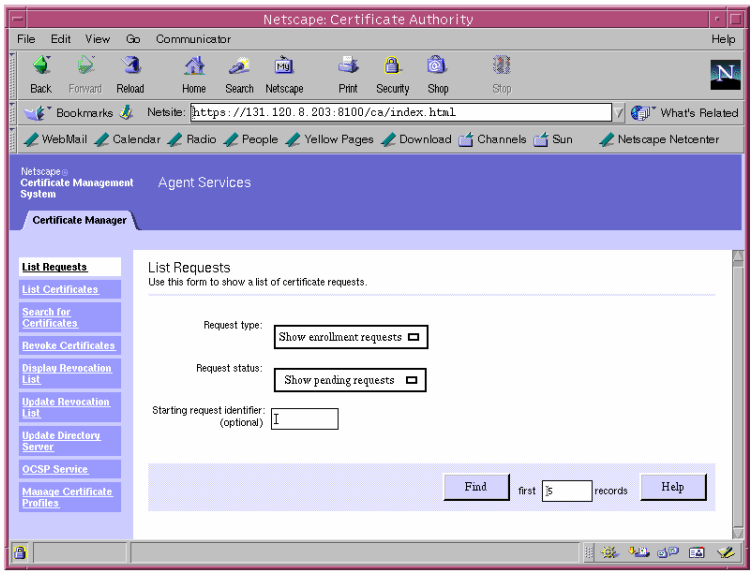
1. Select Data Recovery Manager as the subsystem.

2. Enter the port numbers for both the SSL administration port and the SSL agent port. Make sure that these ports are not already being used by another subsystem or server on the computer.
3. Enter the Key-Pair Information.
    a. Token: internal
    b. Key type: SHA1
    c. Key length: 2048 bits
4. Enter the subject name information for the DRM's certificate.
5. Accept the default certificate extensions.
6. Choose to send the request to a remote CMS now.
    a. Enter the information for the root CA.
    b. Click next.

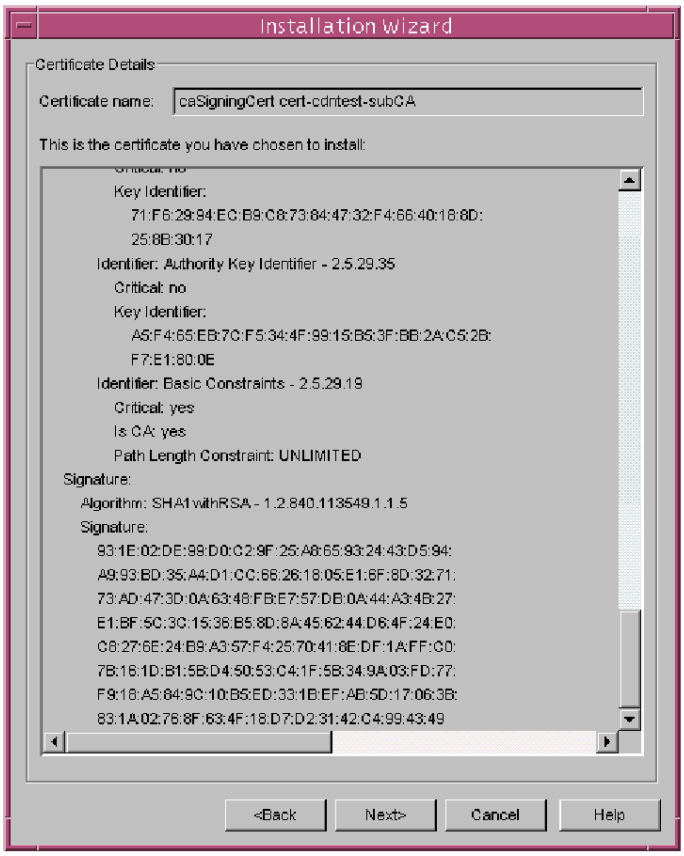


7. In a web browser, go to the agent service page of the root CA., using the port number entered in the CMS instance setup. The browser will prompt for the use of a certificate, select the certificate created for the first agent.

8. On the left side of the page click on list requests.



9. Click Find.
10. Click Details for the request number that was generated in the install.
11. Change the algorithm to SHA1 with RSA.
12. Click Do It.
13. Return to the DRM instance setup.
14. Click next.
15. Select the certificate is at the CMS where your request was sent. The setup program should have forwarded the information to this page. The program will then get the certificate from the CA and install it.



16. Enter the number of recovery agents required and the total number of recovery agents. This can be changed after the installation.

17. Enter the username and password information for the number of recovery agents that were specified.

18. Accept the default key-pair information for the SSL certificate.

19. Enter the subject name information for the certificate.

20. Accept the default certificate extensions for the certificate.

21. Select generate a PKCS10 request.
22. Select send the request to a remote CMS now, using the information for the root CA.
23. Create and install the certificate by repeating steps 7 through 15 listed in this section.
24. Click next.
25. Select to remove the password.conf file.

Registration Manager

1. Enter the information for the root CA.
2. Click yes and enter the information for the Data Recovery Manager.
3. Enter the network configuration information for the RA. Ensure that the ports are not in use.
4. Accept the default Key-Pair information.
5. Enter the subject name information for the RA certificate.
6. Accept the default certificate extensions.
7. Select next.
8. Select send the request to a remote CMS now and enter the information for the root CA.
9. Repeat the step 7 through 15 listed in the Data Recovery Manager section, to create and install the RA certificate.
10. Accept the default key-pair information for the SSL certificate.
11. Enter the subject name information for the SSL certificate.
12. Accept the default certificate extensions.
13. Select generate a PKCS10 request and click next.
14. Again follow steps 7 through 15 from the DRM setup to create and install the SSL certificate for the RA.
15. Select to remove the password.conf file and click next.

16. If you will be using the same user as the agent for the RA as for the CA, you will need to export the certificate from the browser on the CA and import it to the browser on the RA and then copy the certificate information into the user field in the Users and Groups in the RA console. Refer to Chapters 3 – User Certificates and 5 – Users and Groups for more information.

Connecting the Subsystems

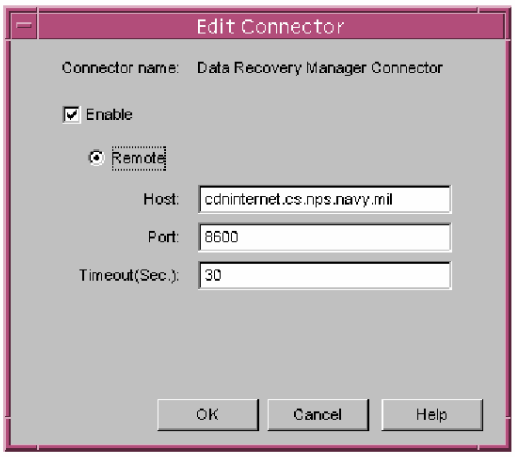
Connectors

In order for the subsystems to talk with one another, the connectors they use must be enabled. The CA must enable its connection to the DRM. The RA must enable its connections to both the CA and the DRM. The steps below discuss how to enable a connection.

1. To set the connections go to the Configuration tab and click the subsystem you wish to connect, RA or CA.

2. Click the connector.

3. Select the connector you want to change then click the Edit tab.



4. Select Enable

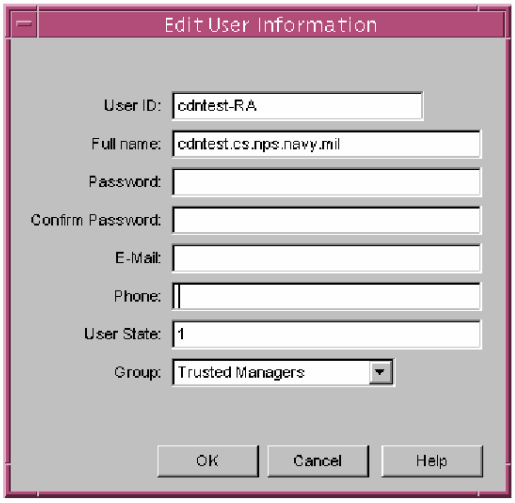
5. Enter the host information and a period in the timeout section. Click OK

6. Repeat for the remaining connections.

Trusted Manager

The Trusted Managers group is a default group whose users are other subsystems that are trusted by this subsystem. For the CA to be able to process requests from the RA, the RA must be a Trusted Manager. For the DRM to process requests from the CA and the RA, they both must be trusted managers. This section will discuss how to add a subsystem as a Trusted Manager. For more information on Users and Groups refer to Chapter 5 of this guide.

1. On the console click the configuration tab. Select User and Groups.
2. Click Add in the Users tab.
3. Fill in the user information as required. The Full Name must be the fully qualified domain name (FQDN). Password, email, and phone information are not required. Leave the User State equal to one.
4. Select Trusted Managers for the group. Click Ok



5. Select the newly created user and click Certificates.
6. Click Import.
7. Go to the end-entity for the CA at: https://cdninternet.npc.navy.mil:1027
8. Click Retrieval tab.

9. Click Find and locate the certificate for the subsystem being setup as a Trusted Manager. Refer to the list below for help in selecting the correct certificate.

    a. RA user on CA – RA signing certificate

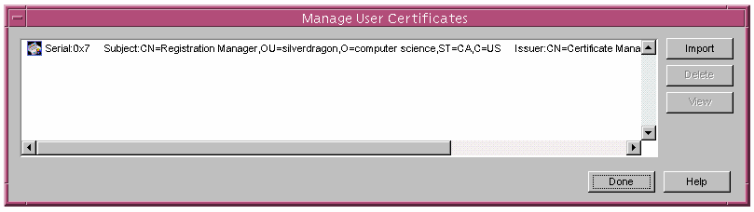
    b. CA user on DRM – CA SSL Server certificate

    c. RA user on DRM – RA signing certificate

10. Copy the base 64-encoding.

11. Go back to the Import Certificate window and click Paste from Clipboard.

12. Click Ok.



13. Click Done.

Adding the KRA Transport Certificate

To be able to perform Key Archival, the certificate enrollment forms must have the DRM Transport Certificate. The certificate must be added to both the CA and RA ProfileSelect.template.

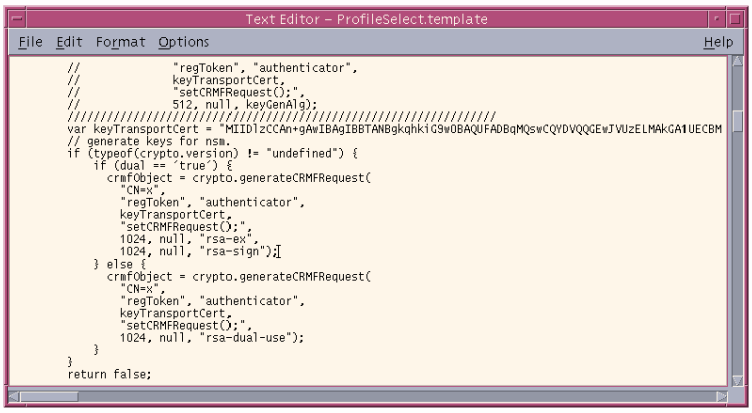
1. Open the agent interface of the CA via a web browser. https://cdninternet.cs.nps.navy.mil:8100

2. Click List Certificates and Find. Navigate to the DRM Transport Certificate.

3. Copy the base 64 encoding for the certificate. Do not include the begin and end certificate tags.

4. Open a text editor and open the ProfileSelect.template located in /usr/netscape/server/cert-cdninternet-CA/web-apps/ee/ca/

5. Paste the certificate into the value for the keyTransportCert variable. Make sure the certificate encoding is surrounded by quotation marks and there are no carriage returns



6. Save the file.

7. Repeat these steps on the computer hosting the RA replacing ra for ca in the directory location.

Chapter 3

User Certificates

Certificate Life-Cycle Implementation

This chapter will define the certificate life-cycle process and how to perform the tasks associated with requesting, issuing, revoking and renewing certificates.

Certificate Issuance

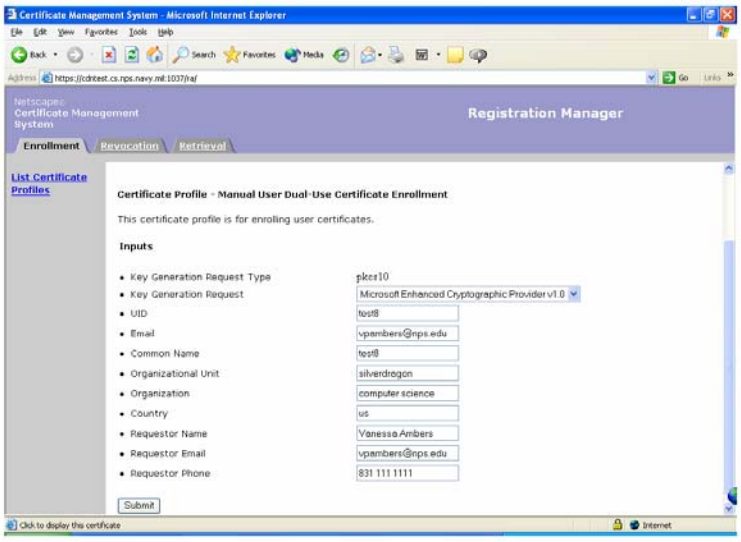
The certificate issuance, approval, retrieval, and renewal portions of this chapter use the interfaces of the RA. They can also be performed using the interfaces from the CA with the correct fully qualified domain name and port numbers.

Owner Request

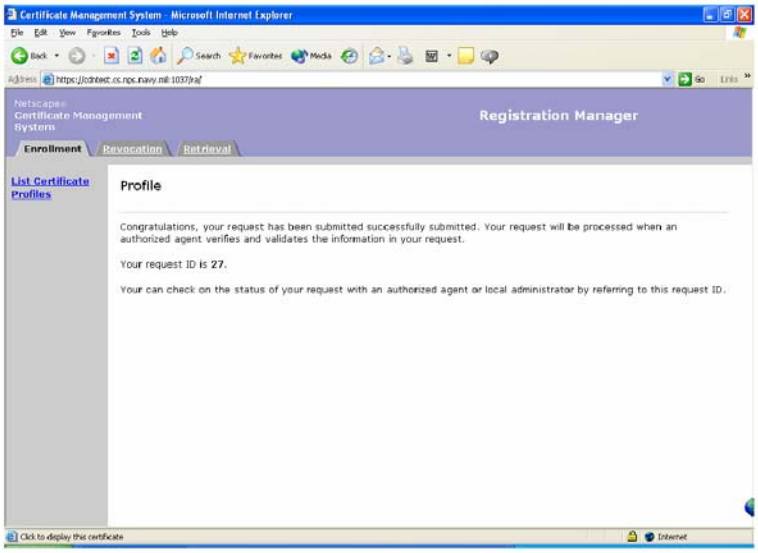
1. On the user machine go to the end entity interface located at: https://cdntest.cs.nps.navy.mil:1037/ra

2. Select the Manual User Dual-Use Certificate Enrollment Form

3. Fill in the information for the PKCS 10 request. If you are using Internet Explorer to generate the keys, select one of the three Microsoft Cryptographic Providers.



4. Click Submit when finished. The next page will provide the requested certificate number.



Request Approval

1. To check the status of the certificate request you must go to the RA Agent Interface at https://cdntest.cs.navy.mil:8800/ra/index.html.

2. Select List Requests from the left hand menu.

3. Click Find.

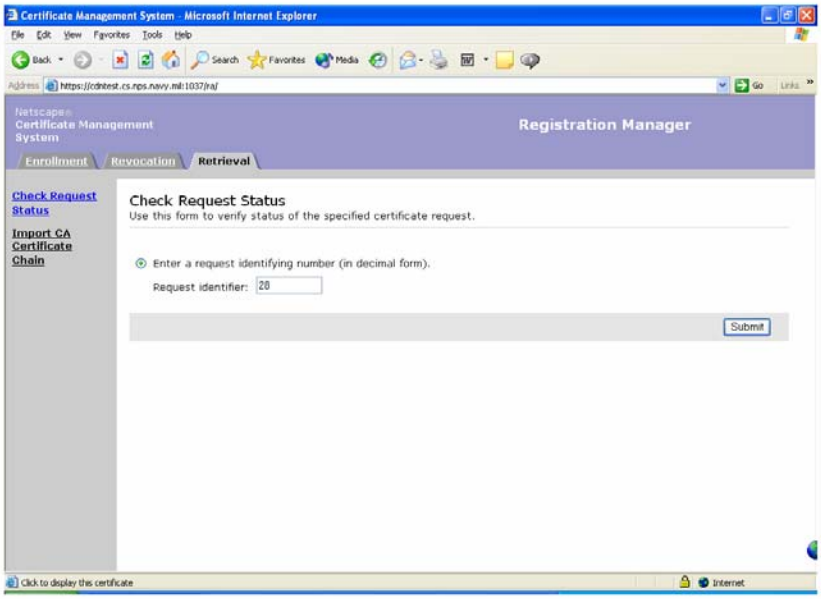
4. Click Details next to your request

5. Look over your certificate for accuracy. Change any information that does violate the constraints of that certificate profile as needed. Scroll to the bottom and tab down to Accept Request (should be default button) and Click Do It.

6. The certificate request will be returned with a request identifying number.

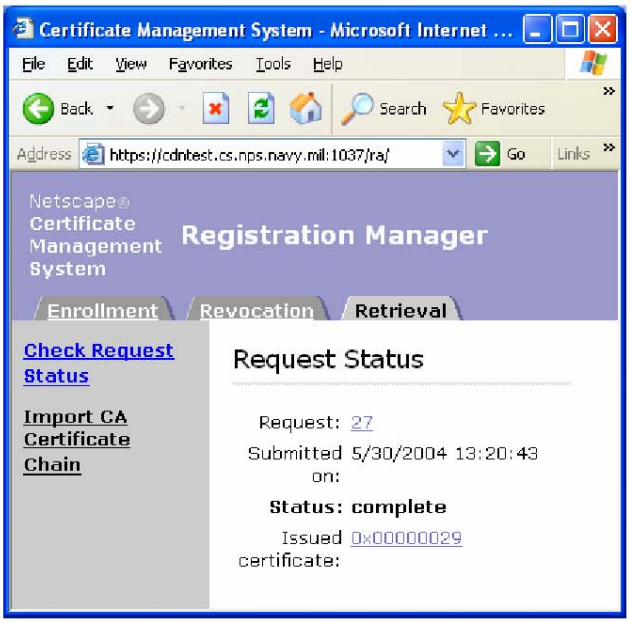
Owner Retrieval

1. On the owner's workstation, click the Retrieval tab at https://cdntest.cs.nps.navy.mil:1037/ra.



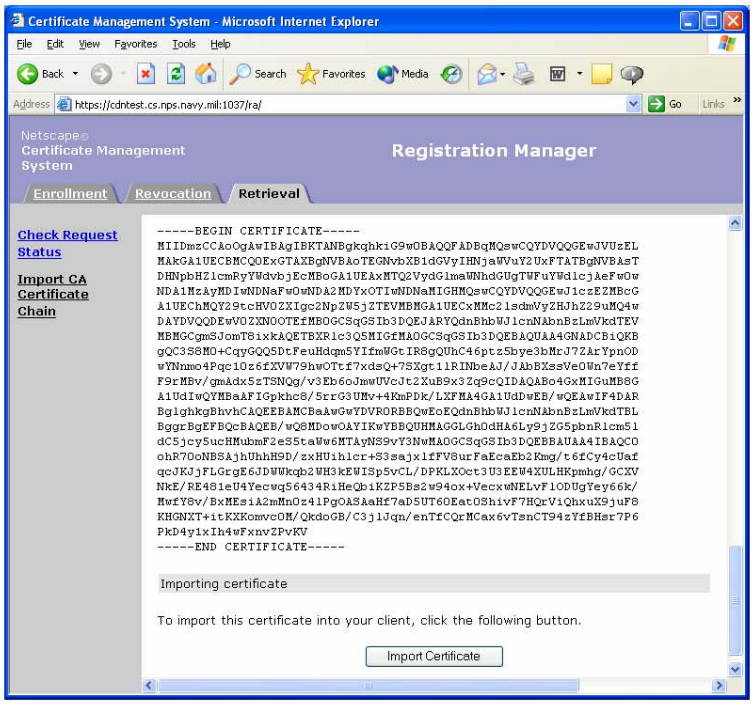
2. Enter the request identifying number provided and click Submit

3. The form will return with a status complete page with the request number and the issued certificate number hyperlinked to the certificate.



4. Click the issued certificate number.

5. Scroll down and view the certificate. If accurate, click import certificate.



Revocation

There are two possible methods for certificate revocation, owner and agent. Owner revocation is done through the SSL end-entity page of either the RA or CA. Agent revocation is done through the agent interface of the CA.

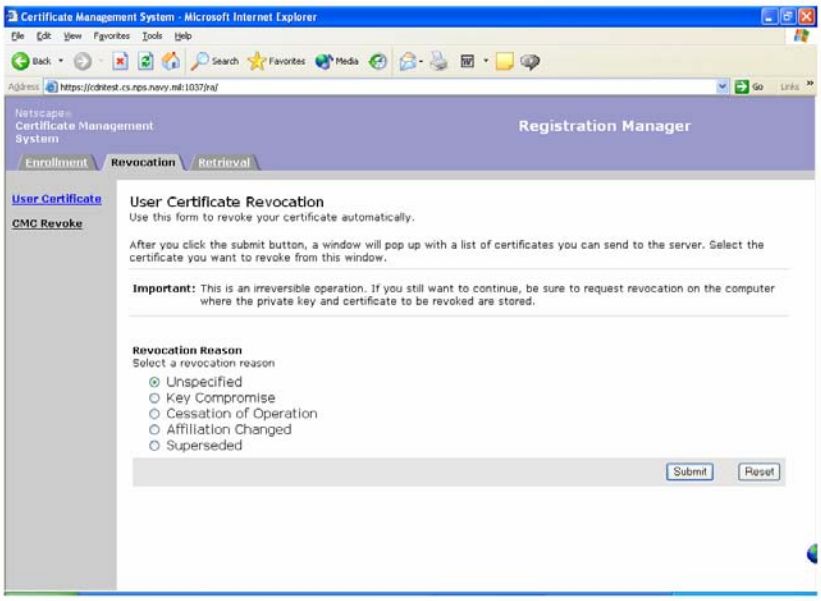
Owner Revocation

1. Go to the SSL end-entity interface for either the RA at https://cdntest.cs.nps.navy.mil:1037 or the CA at https://cdninternet.cs.nps.navy.mil:1027.

2. Click on the Revocation tab.

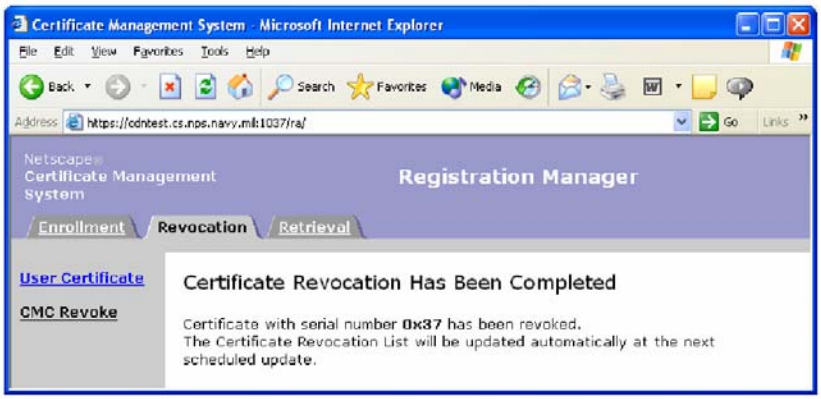
3. The User Certificate Revocation form is the default document shown in the window.

4. Select a reason for revoking the certificate. Click Submit.



5. Select the certificate you wish to revoke from the list in the window that pops up. Click OK.

6. The Certificate Revocation Confirmation page will then appear with the details of the certificate you selected. Fill out any additional information and click Submit.



7. A message will then appear that the revocation has been completed and you will receive an email notification of the certificate revocation.

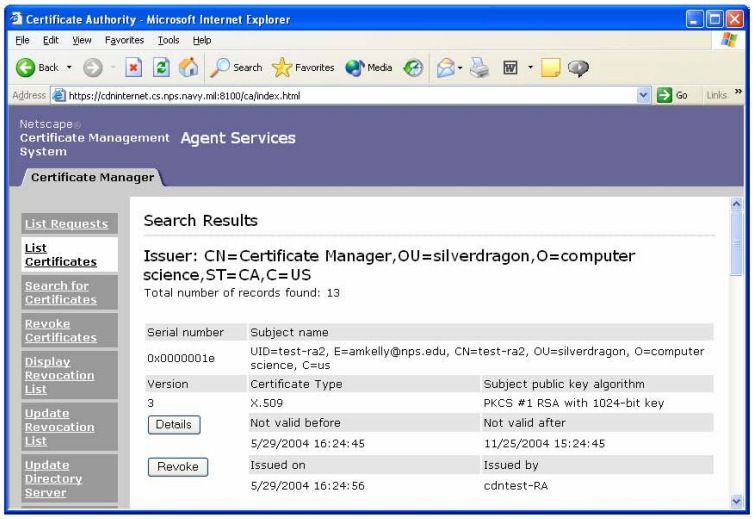
Agent Revocation

Agent Revocation can only be done through the CA's agent interface. There are two methods that can be used to revoke a certificate from this interface, one is through the revoke certificates link and is used mainly for revoking large quantities or by specific characteristics such as validity dates. Upon completion of at least one section of this form, a list of certificates that meet the criteria specified will be displayed including the details and revoke buttons. The second method is through the List Certificates link in the agent interface, where a details button and a revoke button will appear for those certificates the CA can revoke. For each method, the revoke button takes you to the agent revocation page. This section will describe method two, however the majority of this information can be used for both methods.

1. Go to the agent interface of the CA at https://cdninternet.cs.nps.navy.mil:8100.

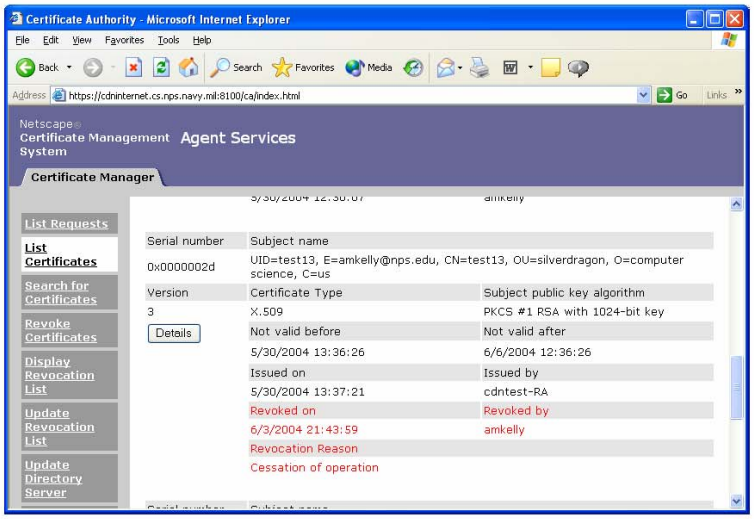
2. Click on List Certificates.

3. Enter the serial number of the certificate you wish to revoke. Click Find.



4. The Certificate Revocation Confirmation Page appears containing the certificate details, an invalidity date area, an area to select the revocation reason and a comment field. Once this information is filled out click Submit.

5. The Certificate Revocation Has Been Completed page will then appear. If you repeat steps 1 through 3, the newly revoked certificate will have red text indicating that the certificate has been revoked.

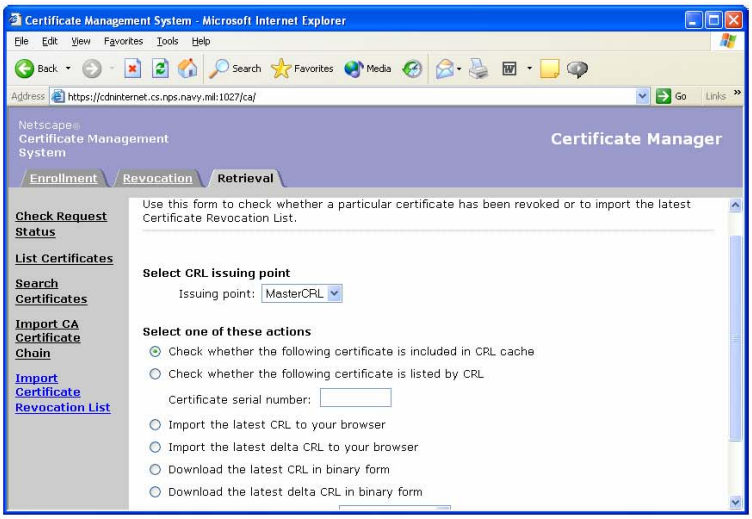


Installing CRL

Currently there is a CRL checking issue with the certificates and Microsoft products. A work around involves importing and installing the CRL manually.

1. Go to the end entity for the Ca at
https://cdninternet.cs.nps.navy.mil:1027/ca/index/html

2. Click the Retrieval tab.



3. Select the Import Certificate Revocation List on the left side.

4. Select the radio button next to Import the latest CRL to your browser.

5. Click Submit.

6. Save the file in the directory of your choice.

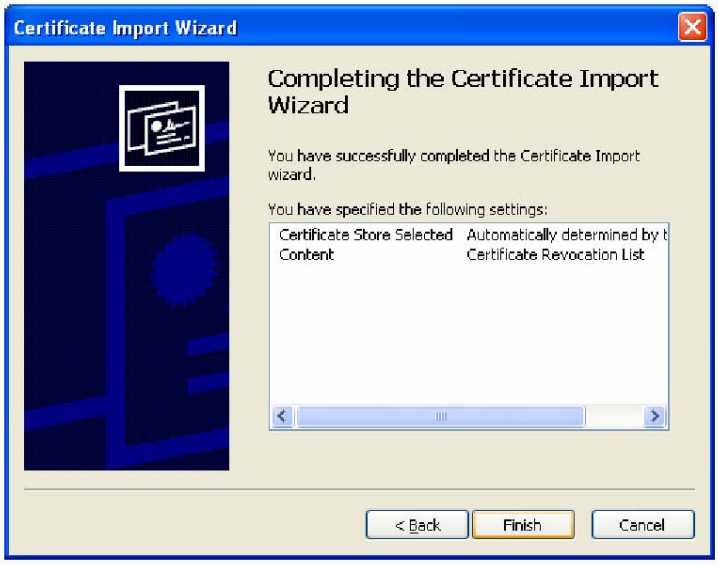
7. Locate the file and right click.

8. Select Install CRL.

9. An Import Wizard will appear, click Next.

10. On the Certificate Store window select the default: automatically select the certificates store based on the type of certificate. Click Next.

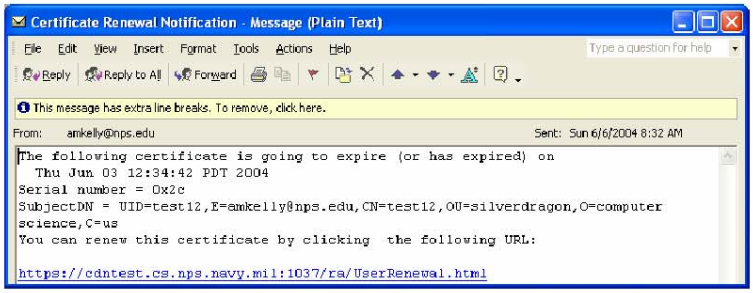
11. The wizard will reply with a status restating the settings you choose. If satisfied click Finish.



12. A message box will appear letting you know the import was successful. Click OK.

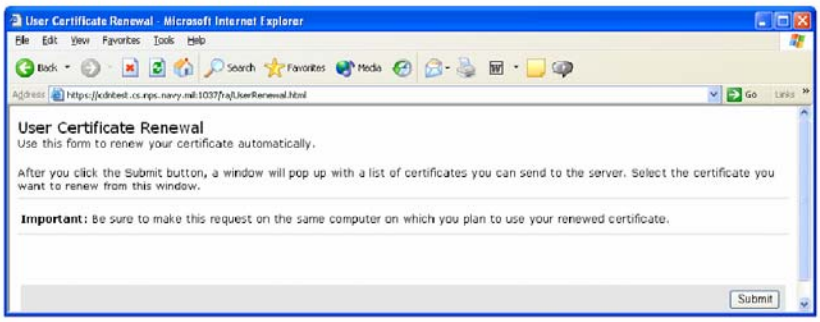
Renewal

1. The user will receive an email stating the certificate number that needs to be renewed with a URL listed.



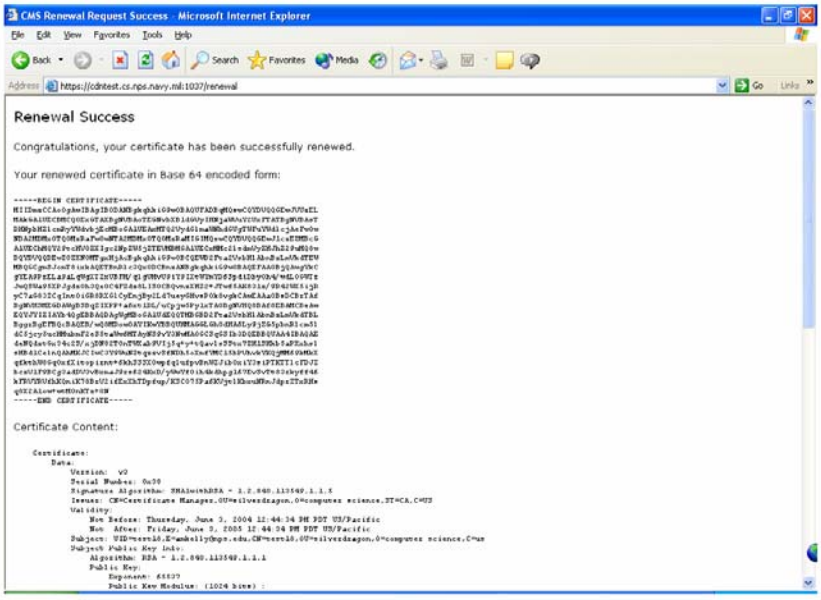
2. Click the URL.

3. Click Submit.



4. A pop up box containing all of the user certificates will appear. Highlight the certificate you want to renew. Click OK

5. A renewal success page will appear with a new certificate for the same subject name with a not valid before date equal to the not valid after date on the old certificate. Click on the import certificate button at the bottom of the page to import the new certificate into your browser.



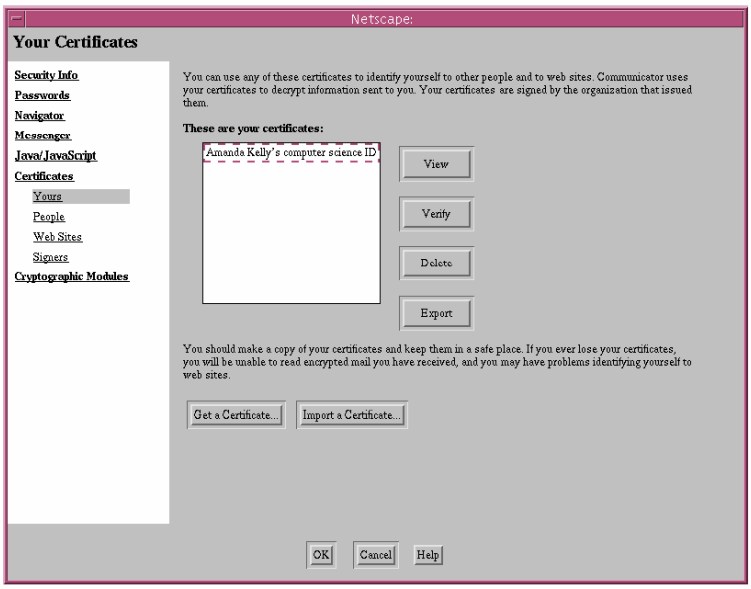
Importing and Exporting Certificate & Keys

As a user moves between workstations or if an agent would like to access the agent interface from a machine other than the one on which the subsystem resides, they must be able to export and import their keys along with their certificate to another browser. The next two sections will discuss how to do this using Netscape. Similar steps can be followed in Internet Explorer.

Export

1. Open a browser window. On the menu bar, click Communicator. Select Tools. Select Security Info.

2. Select Yours underneath Certificates.

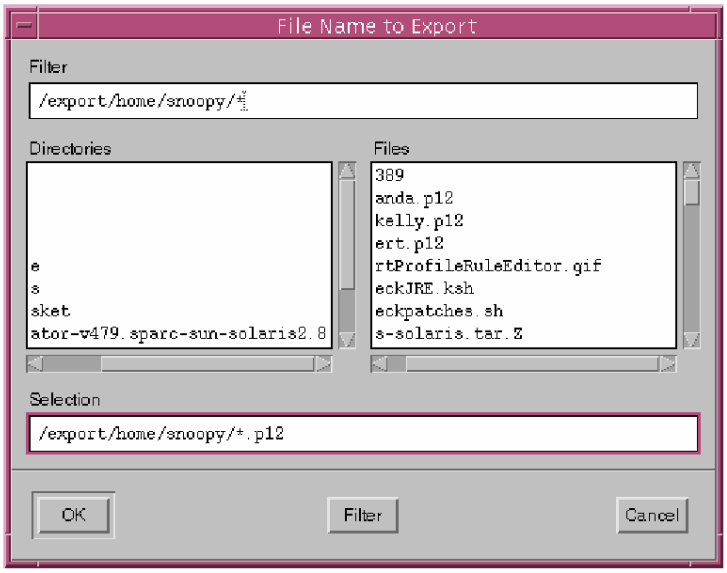


3. Select the certificate you wish to export and click export.

4. Enter the password for the Communicator Certificate DB.

5. Enter the password to protect the data being exported. Reenter the password.

6. Enter the filename of the p12 package and the directory you wish to save it in. Click OK.



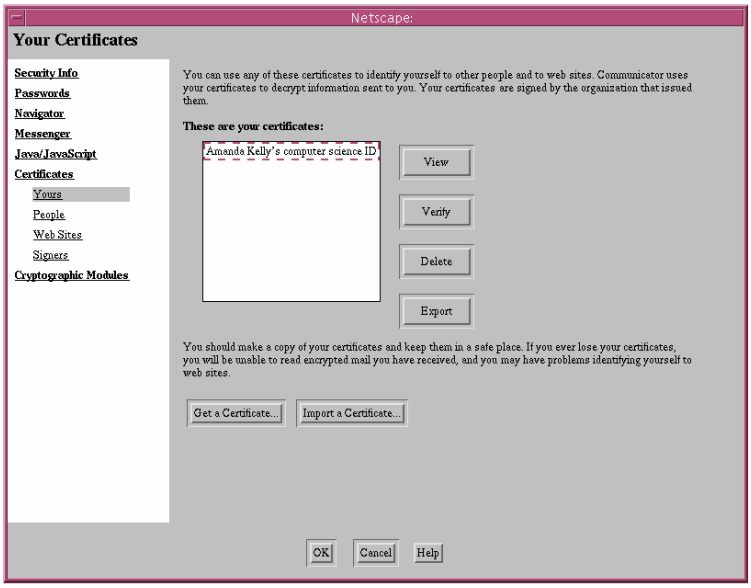
7. Once the export is successful, the p12 file can be transferred to a computer of your choice.

Import

1. Open a browser window. On the menu bar, click Communicator. Select Tools. Select Security Info.

2. Select Yours underneath Certificates.

3. Click Import a Certificate.



4. Select the p12 file you wish to import.
5. Enter the password for the file.
6. You will receive a message that your certificate has been successfully imported.

Chapter 4

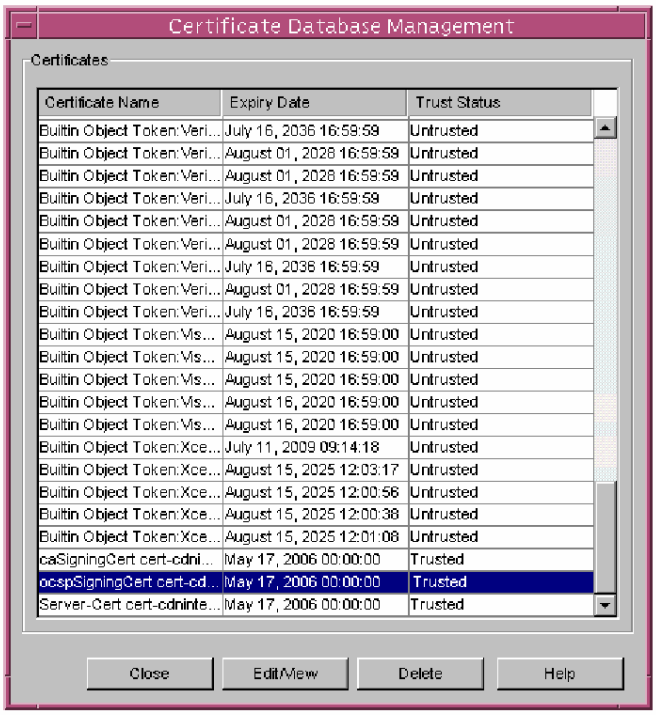
Server Certificates

Managing the Server Certificates of the Subsystems

Managing Certificates

Managing Certificates is used to enable trust relationships with other subsystems in your PKI. Each subsystem should have the root CA certificate listed and the certificate should be trusted. The other certificate listed will depend on the subsystem.

1. Open up Netscape Console for the CA.
2. Click the Configuration Tab.
3. Click on Netscape Certificate Management System on the left side.
4. Select the Encryption Tab.
5. Select Manage Certificates.



6. Scroll to the bottom of the list to view certificates associated with your PKI.
7. Select a certificate and click Edit/View.
8. Click Change to Untrusted/Trusted button to modify the trust of the certificate.

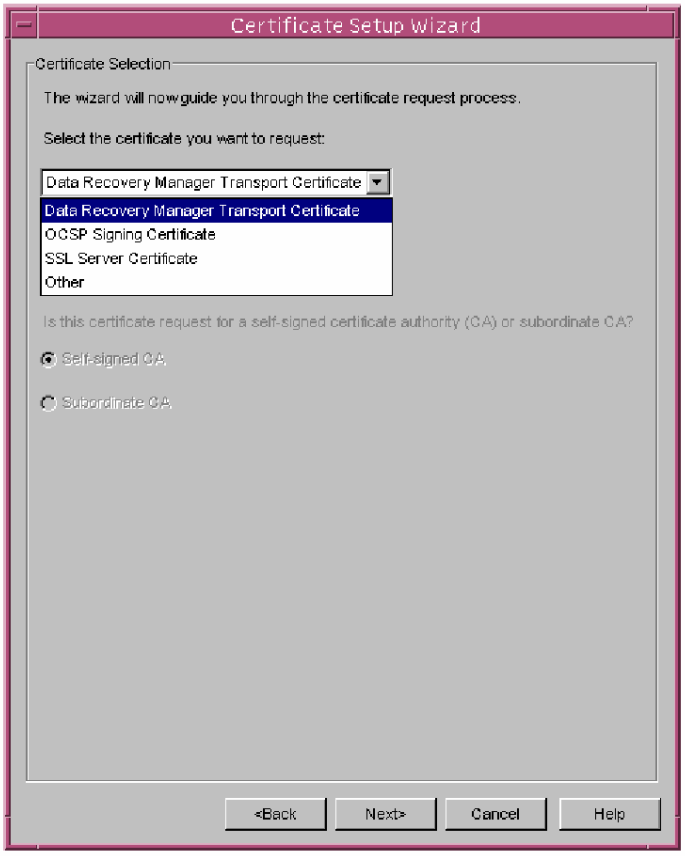
Certificate Setup Wizard

The Certificate Setup Wizard is used for requesting and installing server certificates. On each subsystem, the options available for the type of certificate to request or install listed in the Certificate Selection step depend on the functionality of that subsystem. The steps below are for issuing a new Transport Certificate for the DRM. Theses steps are similar for all of the certificates on all of the subsystems.

Requesting a New Certificate

1. Open Netscape Console for the DRM.
2. Select the Configuration Tab.

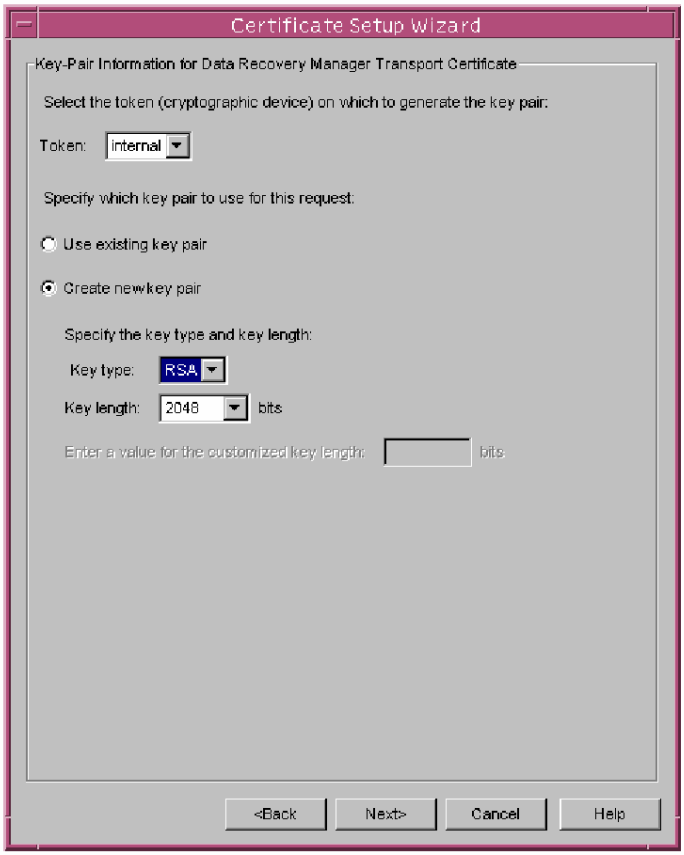
3. Select Netscape Certificate Management System on the left side.
4. Select the Encryption tab on the right side.
5. Click Certificate Setup Wizard.
6. Click Next.
7. Select Request a Certificate.
8. Select the type of certificate you wish to update and click Next.



9. You are then given the options for the Key-Pair Information.

    a. To renew a certificate choose: Use existing key pair.

    b. If the keys were compromised for some reason or you feel new keys are needed, select: Create new key pair.



10. Click Next.

11. Generating the request.

a. If you have selected Create a new key pair, you will be prompted for subject name information. Enter that information and click Next.

b. If you selected Use existing key pair, the wizard has enough information to generate the request automatically. Click Next.

12. Enter the information of the CA to send the request to and click Next.

13. The wizard will return a request number and you must go to the Agent Interface of the CA and approve the request. Refer to the Request Approval section in Chapter 4 of this guide.

14. Click Done.

Installing a New Certificate

1. Open Netscape Console for the DRM.

2. Select the Configuration Tab.

3. Select Netscape Certificate Management System on the left side.

4. Select the Encryption tab on the right side.

5. Click Certificate Setup Wizard.

6. Click Next.

7. Select Install a certificate and click Next.

8. Select the type of certificate you wish to install and click Next.

9. Go to the agent interface of the CA (https://cdninternet.cs.nps.navy.mil:8100). Navigate to the certificate you just approved. Copy the base 64 encoding including Begin Certificate and End Certificate.

10. Select the certificate is located in the text area below. Click Paste from Clipboard.

11. Click Next.

12. Click Done.

13. Return to Manage Certificates and ensure that the certificate that you just installed is trusted. Also remember that you will have to adjust the ProfileSelect.template files on both the CA and RA for key archival requests (Chapter 2 – Adding the KRA Transport Certificate

Chapter 5

Users and Groups

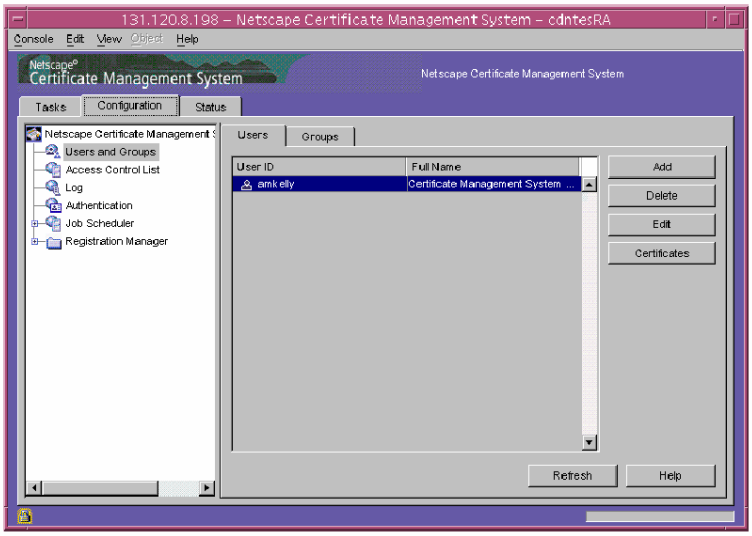
Managing Users and Groups

Users

Users, based on the groups to which they are assigned, have access to specific areas of the Netscape Console and web interfaces of a subsystem.

Add

1. Open the console for the subsystem.
2. Select User and Groups. Click Add

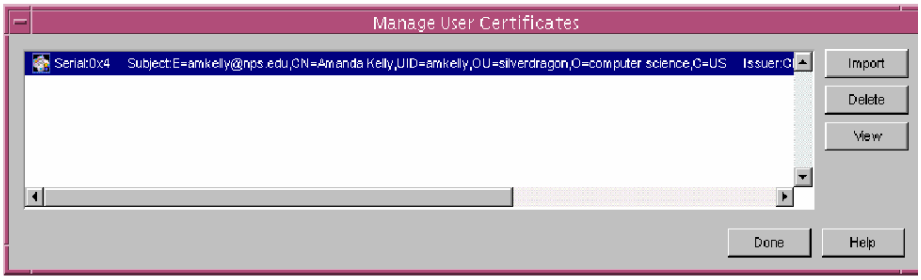


3. The Edit User Information window will appear, add the information needed. You do not have to enter a password, email address or phone number. Select the group to which they will belong initially.

4. Click OK. You can then edit user information via the edit button.

5. Next you need to add the user's certificate to the user information for authentication purposes.

6. Select the User and click Certificates.

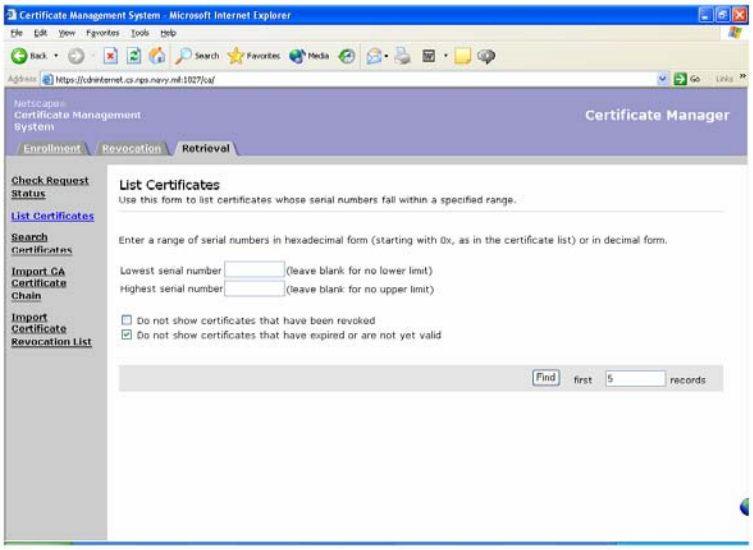


7. Select the Import key.

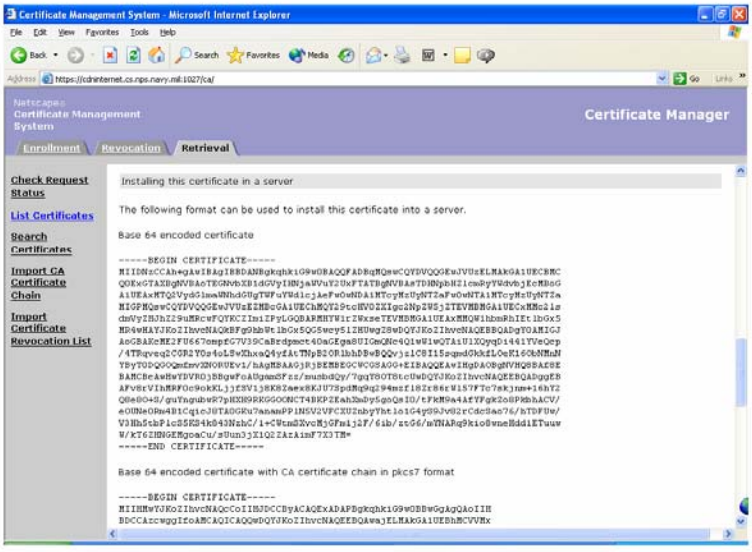
8. Go the CA end-entity interface at: https://cdninternet.cs.nps.navy.mil:1027/ca

9. Click the Retrieval tab.

10. Go to List Certificates and enter the certificate number or click Find. Select the certificate associated with this user.



11. Copy the base 64 bit encoding from the certificate.



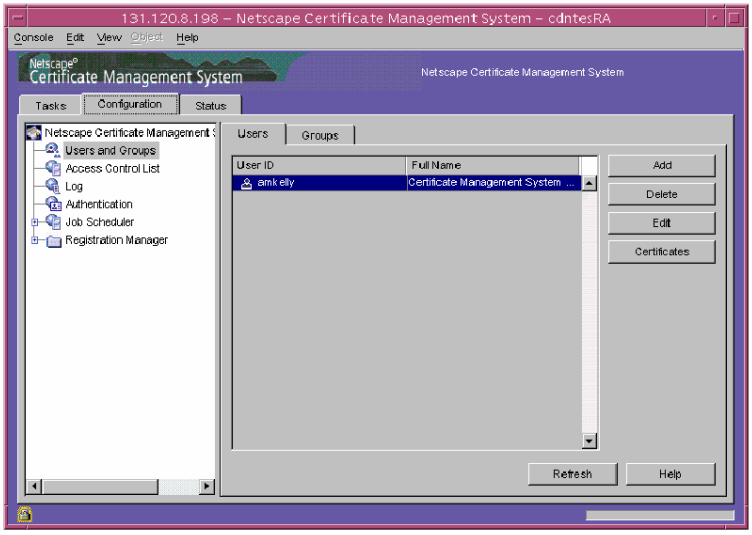
12. Return to the Import Certificate window and click Paste from clipboard. Click OK.

13. The certificate will appear in the Manage User Certificates window. Click View to view the certificate if desired and then click Done.

Delete

1. Open the console window for the subsystem.

2. Select Users and Groups. Select the user you want to remove and click Delete



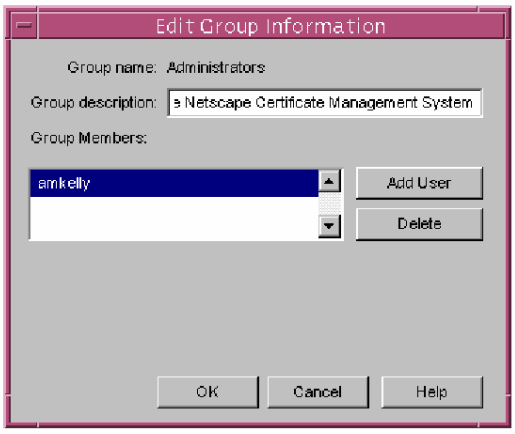
3. A warning message will appear verifying you want to remove a user. Click Yes.

Groups

Add

1. Open the console window for the subsystem. Select Users and Groups.

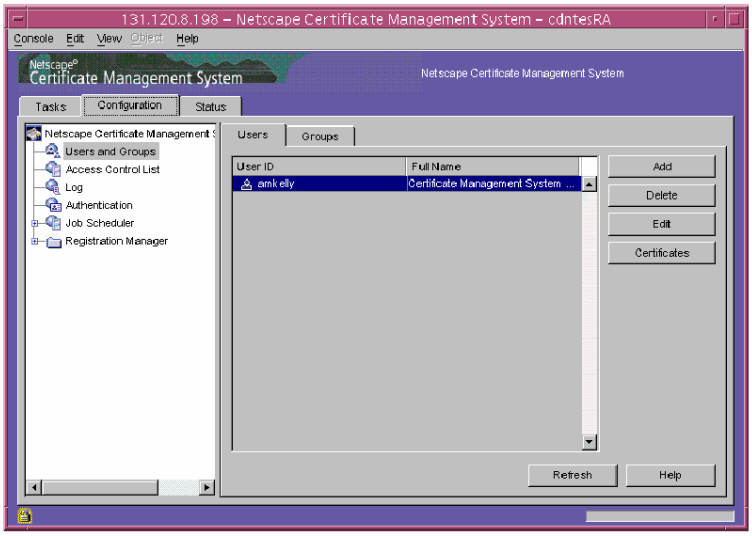
2. Click on the Groups tab. Users is the default selection. Select the Add key.



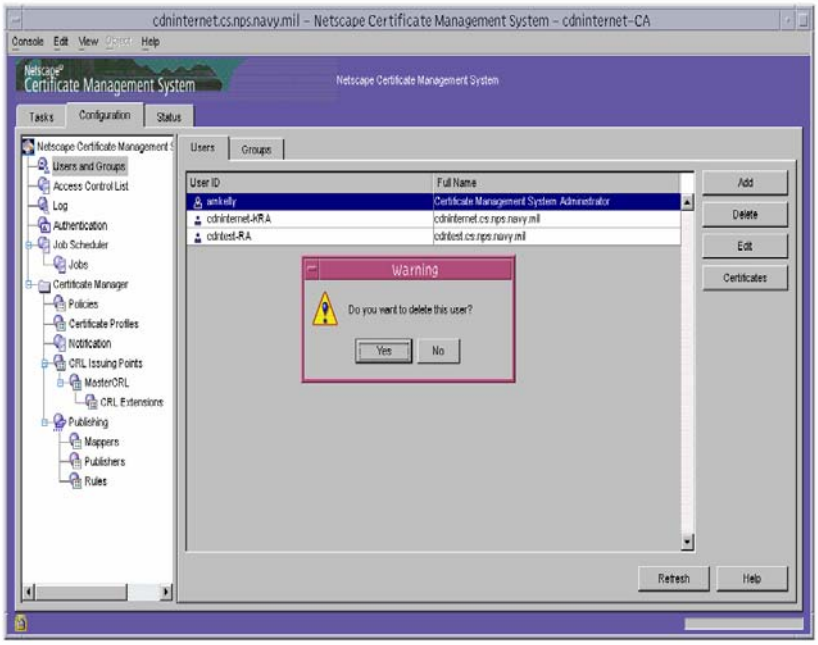
3. An Edit Group Information window will pop up. Add the needed information to include the user associated with the group. Click OK

Delete

1. Open the console window for the subsystem. Select Users and Groups.



2. Click on the tab for Groups. Select the group you want to remove and click Delete.



3. A warning message will appear verifying you want to remove the selected group. Click Yes.

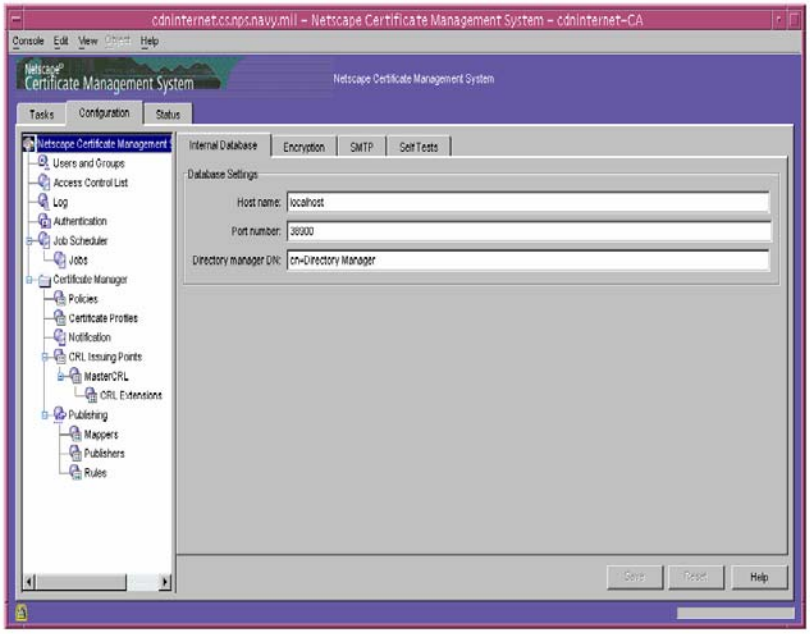
Chapter 6

Notification and Jobs

Setting up notifications and jobs

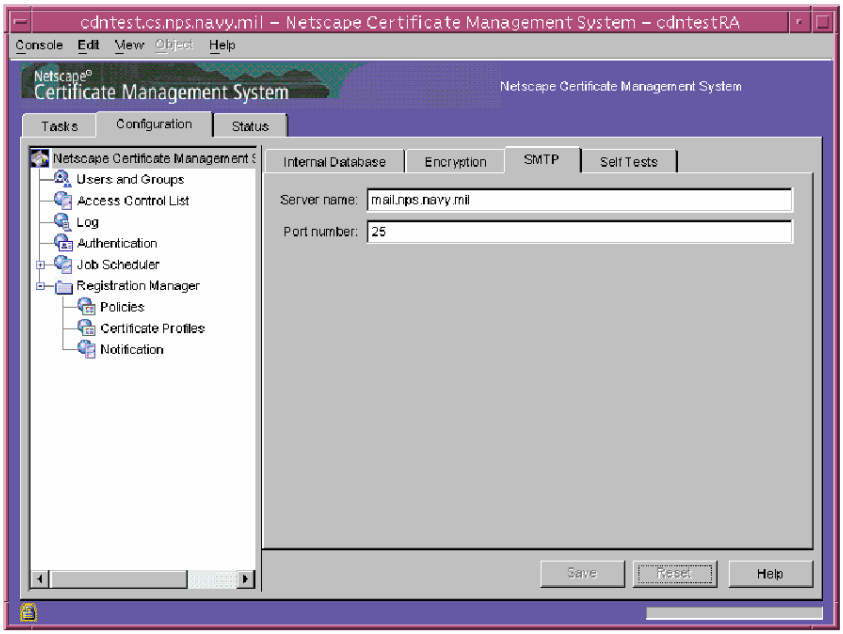
Setting Up the Mail Server

1. Open up the console for the CA.
2. In the left hand panel select Netscape Certificate Management System.



3. In the right hand panel click the SMTP tab.

4. Enter the email server and port number.



5. Click Save.

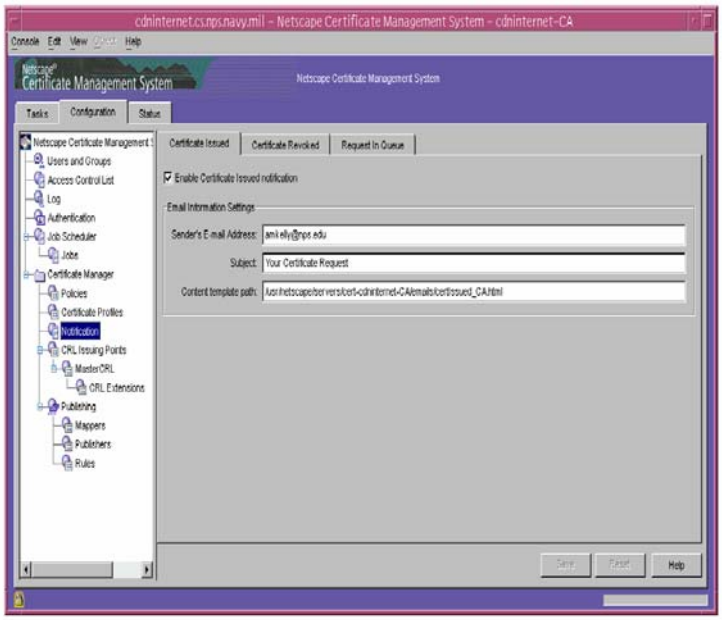
6. This should be repeated for the RA as well.

Enabling Notifications

1. In the console, expand the list under Certificate Manager.

2. Select Notification.

3. There are three possible notifications listed: Certificate Issued, Certificate Revoked, and Request in Queue.



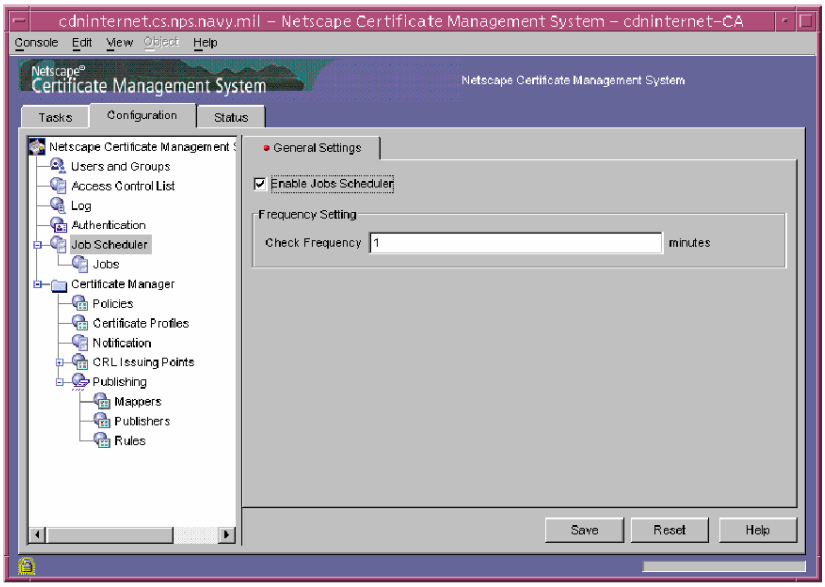
4. For each notification select its tab, click the enable box, and enter in the information needed. To have a notification go to more than one user separate the email addresses by commas.

5. Click Save for each tab.

This can be repeated for the RA as well, by replacing Certificate Manager with Registration Manager. The RA only has the Certificate Issued and Request in Queue notifications since it does not have the authority to revoke certificates.

Job Scheduler & Jobs

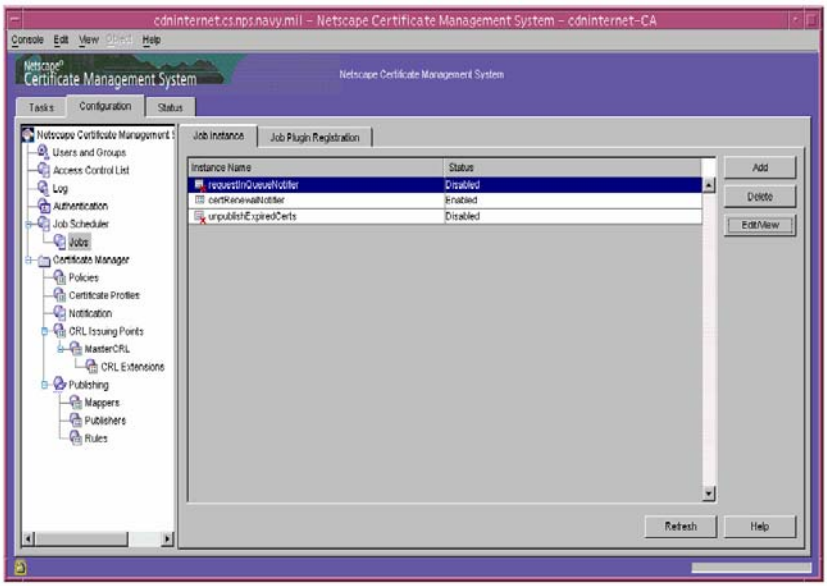
1. To use Jobs, you must first enable the Job Scheduler by selecting Job Scheduler on the left hand side of the console.



2. Check the Enable Jobs Scheduler box.

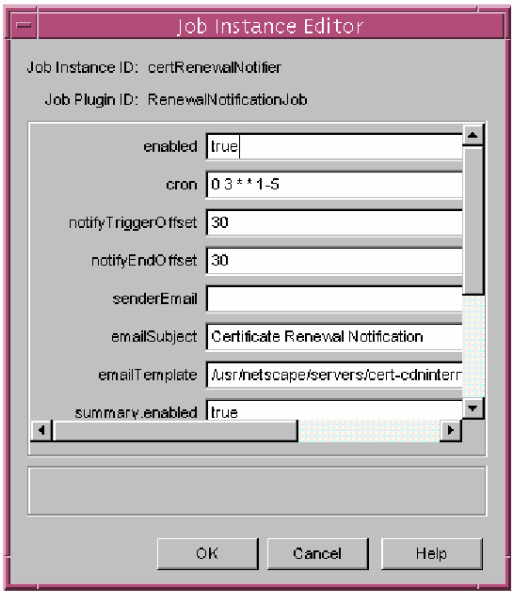
3. Enter the frequency in minutes that the scheduler should check for awaiting jobs to be processed.

4. Expand the Job Scheduler on the left side panel.



5. Select Jobs. From here you can either add or delete a job instance or edit/view an existing job instance.

6. To edit a job instance click the Edit/View button. A window will appear with blank fields. Input the required information.


Job Instance Editor
Job Instance ID: certRenewalNotifier
Job Plugin ID: RenewalNotificationJob
enabled
true
cron
0 3 * * 1-5
notifyTriggerOffset
30
notifyEndOffset
30
senderEmail
emailSubject
Certificate Renewal Notification
emailTemplate
/usr/netscape/servers/cert-cdninterr
summary.enabled
true
OK
Cancel
Help

7. Click OK.

Chapter 7

Certificate Profiles

Managing the aspects of Certificate Profiles

Certificate Profiles are used by the CA and the RA for the creation of certificates for your organization. Each profile can be setup for a specific type of user or system. The profiles contain certificate extension information and the inputs and outputs required for that type of enrollment. Once a profile has been created, an HTML page is created for the end-entity interface. A user can then access that enrollment page for that certificate profile by selecting it in the Enrollment Tab. This chapter discusses the management of Certificate Profiles.

Approve or Disable a Profile

1. Open a browser to the agent interface of the CA. https://cdninternet.cs.nps.navy.mil:8100

2. Click Manage Certificate Profiles

3. Select a Profile.

4. At the bottom of the page is either an Approve or a Disable button. This toggle button allows for a profile to be approved, meaning that it is accessible via the end-entity interface, or disabled, meaning that it is not accessible from the end-entity page. A profile must be disabled before an administrator can modify it in the Netscape Console.

Adding a Certificate Profile

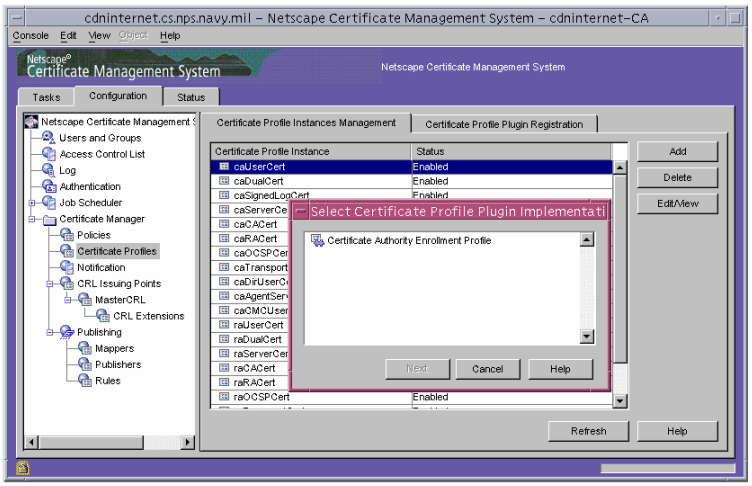
A quick note: for certificate enrollment initiated through the RA, the CA must have a copy of the certificate Profile, with the same name, used by the RA. As mentioned in step six below, the profile for the RA will have End User Certificate Profile set to true. The same profile on the CA will have End User Certificate Profile set to false, ensuring that the request does not have to be processed via the input form associated with that profile on the CA.

1. Open the Netscape Console of the CA.

2. Expand the Certificate Manager list on the left side.

3. Select Certificate Profiles.

4. Click Add under the Certificate Profile Instances Management tab.

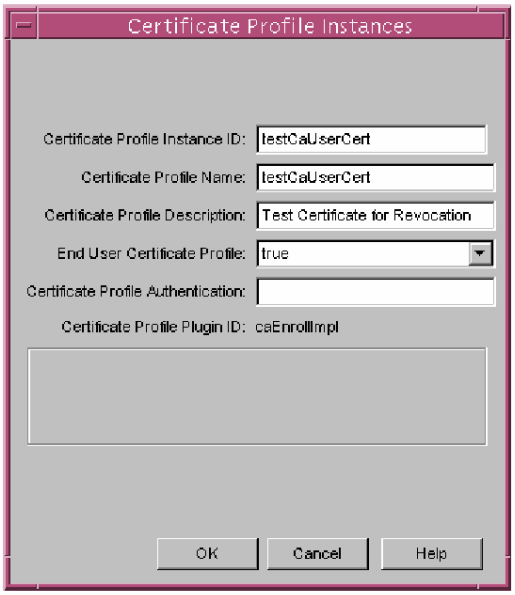


5. Select Certificate Authority Enrollment Profile and click Next.

6. Enter the information requested and click OK.

    a. If this profile is to be used only by the CA, End User Certificate Profile should be set to true.

    b. If this profile is a duplicate of a profile that will be used by the RA, then End User Certificate Profile should be set to false. In the same profile on the RA, this value will be set to true.



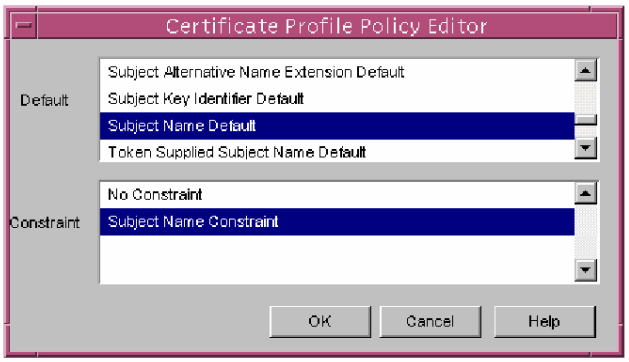
7. The profile will then appear in the profile instance list and is ready to be configured using the Edit/View button. Select the profile and click Edit

8. Select the Policies tab and click Add. A list of possible certificate extensions will appear. For each extension needed by for this certificate type, repeat the following steps. For more information on Certificate Extensions go to the Administrator's Guide, Netscape Certificate Management System, Version 6.1, page 717.

    a. Select the Extension.

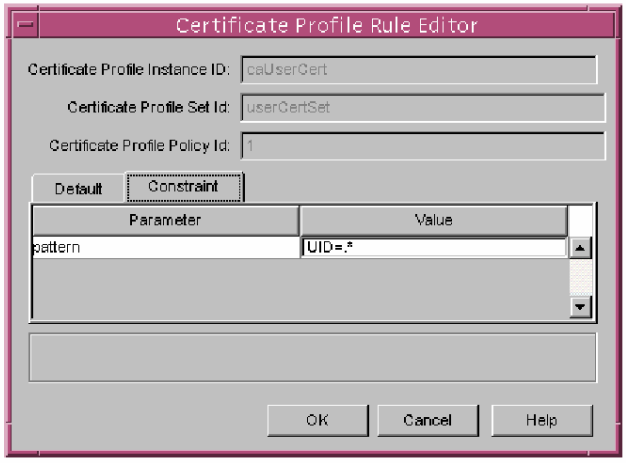
    b. Select No Constraint or Extension Constraint. Only one choice may appear in the bottom portion of the window, in that case select the default. Each extension can have different constraint possibilities. Refer to the Administrator's Guide listed above for more information.

    c. Click OK.

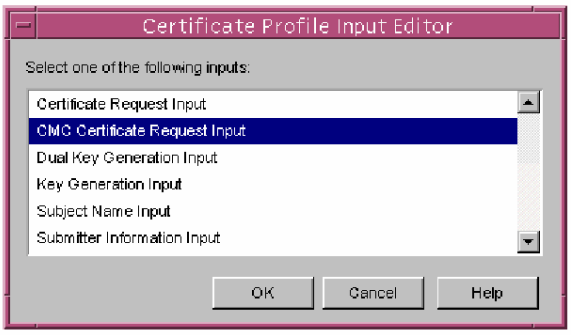


d. Enter a Policy Set Id and a Policy Id.

e. Fill out the information relevant for the extension under the Default and Constraint tabs. Click OK when finished.



9. Select the Inputs tab and click Add. Select on of the six possible inputs and click OK.



a. Enter the Id and click OK

b. Repeat for all of the inputs required.

10. Click on the Outputs tab. Currently, there is only one possible output. Select Certificate Output, enter the Id and click OK.

11. Click OK.

12. Return to the agent interface of the CA.

13. Click Manager Certificate Profiles.

14. Select the profile you just added.

15. Click Approve. The profile is now available for certificate enrollment by the user.

Editing a Certificate Profile

1. Complete the steps in Approve or Disable a Profile above to disable the profile you wish to edit. A profile must be disabled to be modified.

2. Open the Netscape Console of the CA.

3. Expand the Certificate Manager list on the left side.

4. Select Certificate Profiles.

5. Select the profile you wish to edit and click Edit/View.

6. At the Policies, Inputs, and Outputs tabs, you can delete or edit any of the Ids currently listed or you can add a new Id.

7. Click OK when you are finished making modifications.

8. Repeat step 1, to approve the profile.

Deleting a Profile

1. Complete the steps in Approve or Disable a Profile above to disable the profile you wish to edit. A profile must be disabled to be deleted.

2. Select the profile you wish to delete.

3. Click the Delete button.

4. You will be prompted "Are you sure you wish to delete this profile?" Click Yes.

Chapter 8

Publishing and CRL Issuing Points

Enabling and configuring publishing and CRL Issuing Points

The Certificate Authority is the sole authority of the CRL in CMS PKI. Only CA agents can revoke certificates and only CA administrators have the authority to configure CRL issuing points and enable CRL publishing to the Directory Server.

Configuring the CRL Issuing Point

1. Open Netscape Console for the CA.
2. Expand the Certificate Manager List.
3. Expand the CRL Issuing Points. If you select CRL Issuing Points, a list of CRL issuing points will be displayed. From here you can add, edit, or delete an issuing point.
    a. To Add
        i. Click Add
        ii. Check enable
        iii. Enter the name and description of the issuing point
        iv. Click OK
    b. To Edit
        i. Click Edit
        ii. Check or uncheck enable
        iii. Modify the description if needed.

iv. Click OK

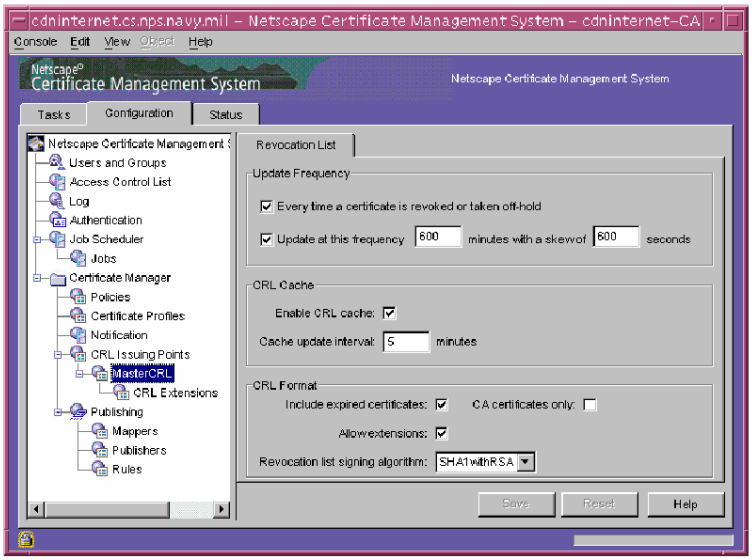
c. To Delete

i. Select the Issuing Point you want to delete.

ii. Click Delete.

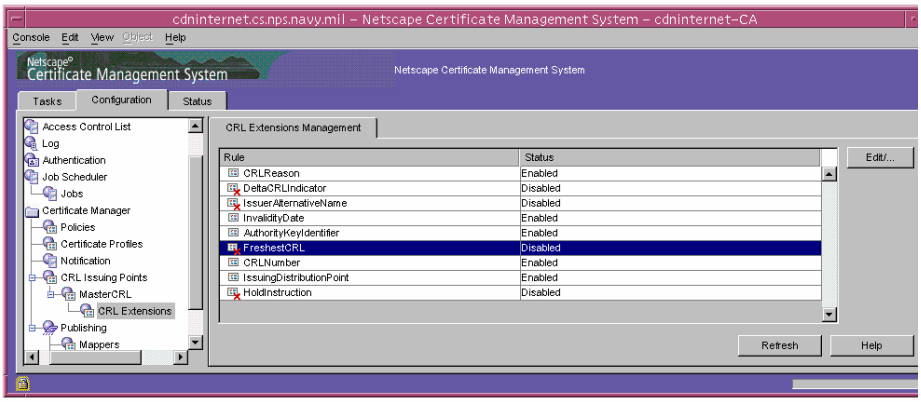
iii. Click Yes.

4. Select the Issuing Point. From here you can modify the update frequency, the CRL cache information, and the CRL format. After making any needed changes, click Save to apply them.



5. Expand the Issuing Point.

6. Select CRL Extensions.

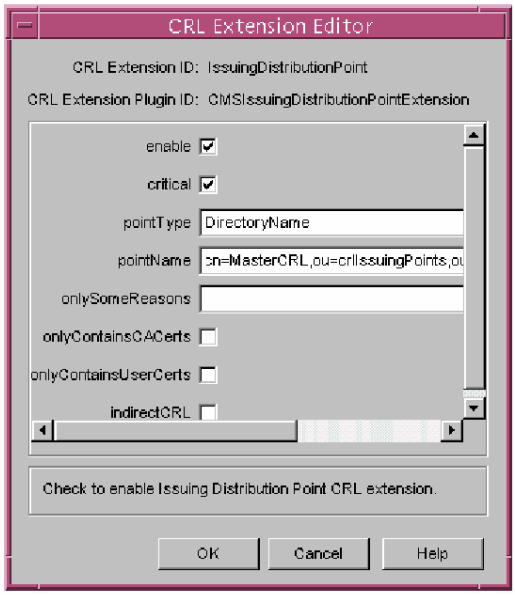


7. Select the extension you wish to modify. Click Edit/View.

    a. Check or uncheck enable.

    b. Check or uncheck critical.

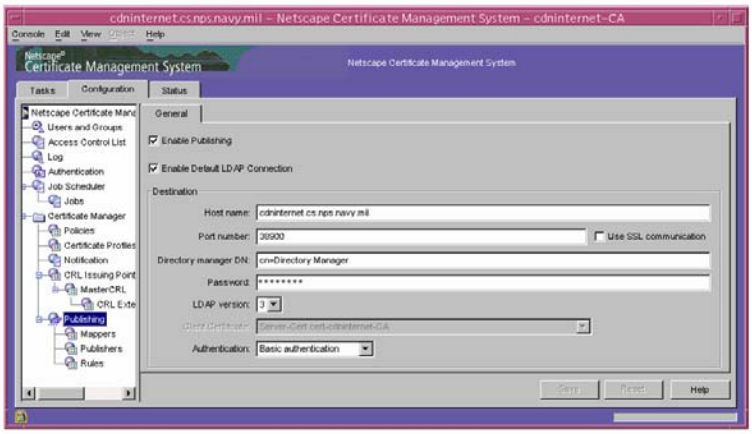
    c. Add or modify other information relevant to that particular extension.



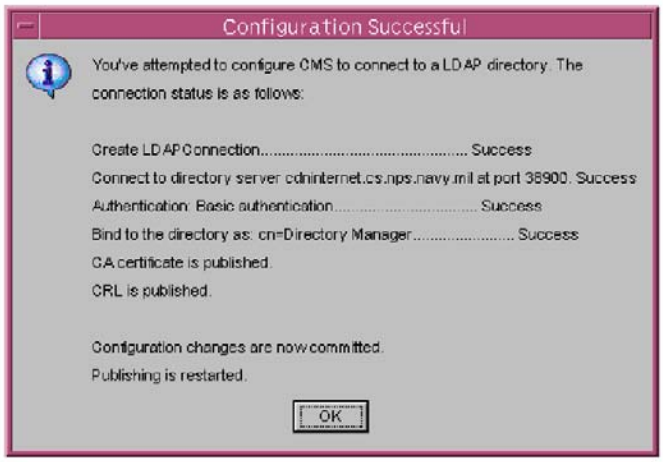
Publishing

Enabling publishing allows certificates and the CRL to be published to the Directory Server allowing for LDAP connections to retrieve that information.

1. Open Netscape Console for the CA.
2. Expand the Certificate Manager list.
3. Select Publishing.
    a. Click Enable Publishing.
    b. Click Enable Default LDAP Connection and enter in the information for the Directory Server Instance (cdninternet-CA-db) in the CA's server group.



c. Click Save. A series of Java communications are performed with the Directory Server. If all of the tests were successful then the following image will appear. If the tests were not successful and an error occurred you will need to check the log files (Select the Status tab, expand the log list, select system) to determine what the error was.



There are three more components to publishing; mappers, publishers, and rules. They can be added, configured and deleted as needed. The default values installed in those components during the initial installation did not require modification for this thesis.

For more information on publishing refer to Administrator's Guide Netscape Certificate Management System, Version 6.1, page 617.

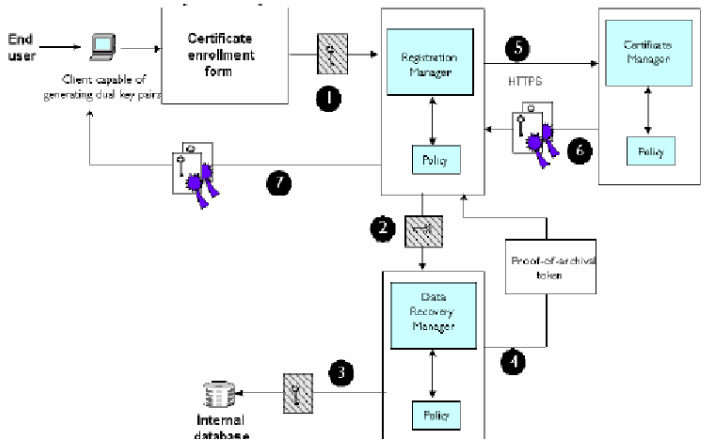
Chapter 9

Key Archival and Recovery

Managing Key Archival and Recovery

Key Archival

Assuming that all of your trust relationships, trusted managers, users, and ProfileSelect.templates are setup up correctly, key archival should be a simple process that occurs during certificate request. The certificate owner must generate the request from a Netscape 7.1 browser or higher and the key generation type must say CRMF. Once the request is made, the owner will be prompted to approve the transport of their private key, encrypted by the DRM Transport Certificate. Once the certificate is created, the keys and certificate will be sent to the DRM for storage. This information is stored in the Directory Server of the DRM, encrypted by its Storage Certificate. At the time of this writing, there is a problem with the trust relationships between the CA and DRM, so key archival is inoperable. Therefore no other information on it can be provided. Below is the key archival process as described in the Administrator's Guide.

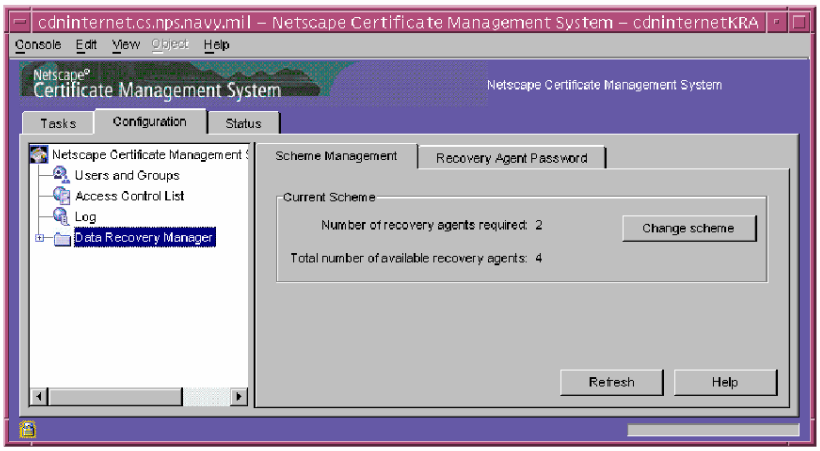


Key Recovery Scheme

Archived keys remain encrypted until key recovery agents use passwords to unlock the password-splitting mechanism. The Administrator's Guide states:

> For the protection of the storage key pair, the Data Recovery Manager supports a password-splitting mechanism called *m of n secret splitting or sharing*, whereby it splits the PIN that protects the token in which the storage key pair resides among *n* number of key recovery agents and reconstructs the PIN only if *m* number of recovery agents provide their individual passwords; *n* must be an integer greater than 1 and *m* must be an integer less than or equal to *n*.[1]

During the DRM subsystem installation, the administrator selects the m of n scheme, where m is the number of recovery agents required to unlock the storage key and n is the number of possible recovery agents as seen below. Both the scheme and the recovery agents' passwords can be modified.

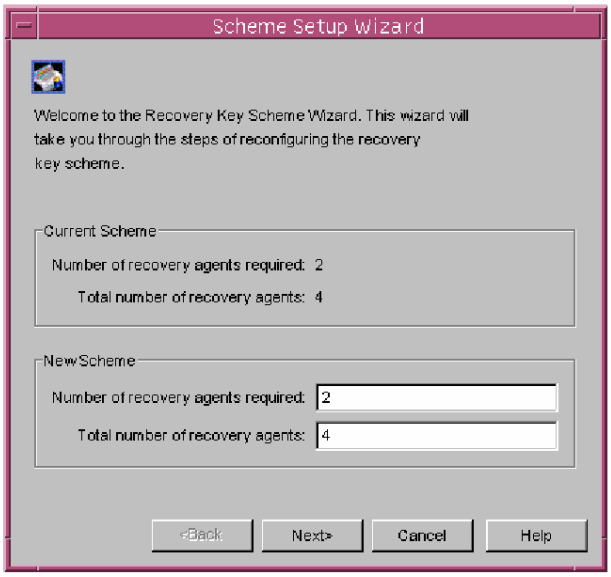


Scheme Management

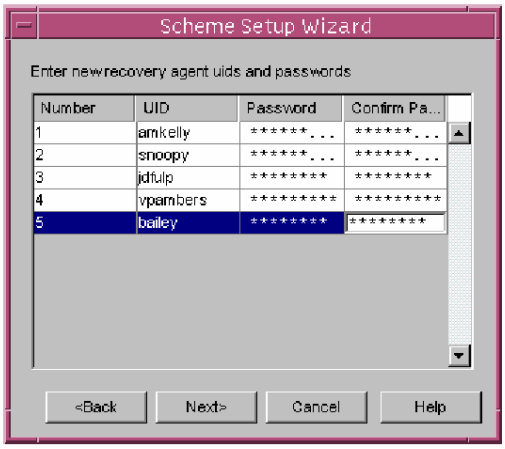
1. Open Netscape Console of the DRM.
2. Select the Configuration tab.
3. Select Data Recovery Manager on left side.
4. Select Scheme Management tab on right side.

[1] Administrator's Guide, Netscape Certificate Management System Version 6.1, Feb 2003, pg 206.

5. Click Change scheme.
6. Enter the new numbers for number of recovery agents required and total number of recovery agents.



7. Click Next.
8. Enter current recovery agent UIDs and passwords.
9. Click Next.
10. Enter the UIDs and passwords for all of the available recovery agents.



11. Click Next.

12. Click Done.

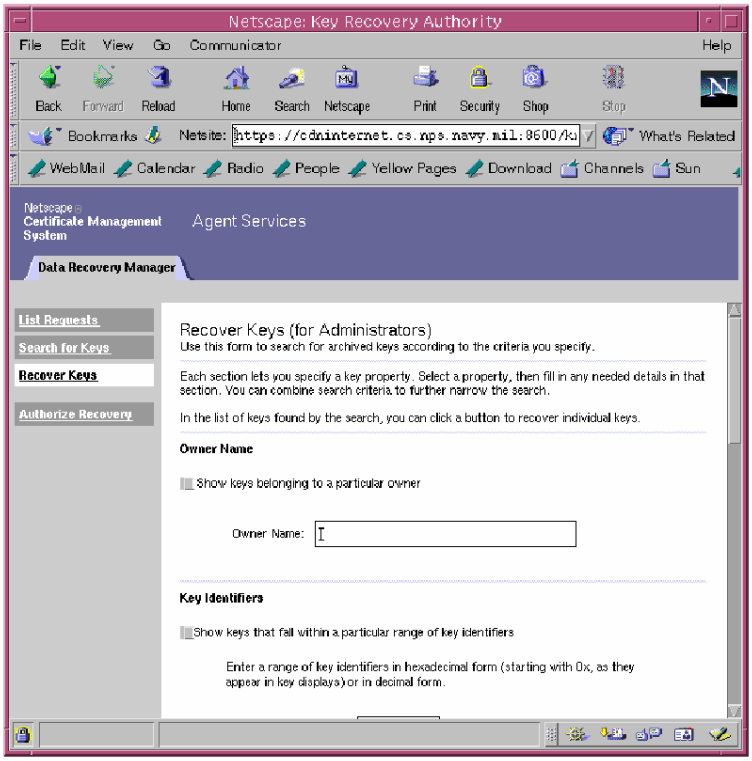
Changing Recovery Agent Passwords

1. Open Netscape Console of the DRM.
2. Select the Configuration tab.
3. Select Data Recovery Manager on left side.
4. Select Recovery Agent Password tab on right side.
5. Select the Recovery Agent for whom you would like to change the password.
6. Click Change password
7. Enter old password and the new password twice.
8. Click OK.

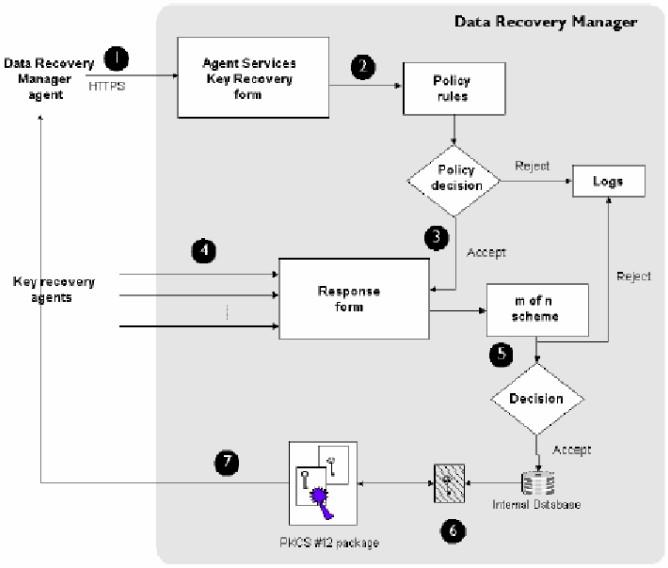
Note: Changing the recovery agent passwords should be done directly after the installation of the DRM and on a recurring basis (every 6 months) after that. There should also be a policy on the composition of the passwords (length, numbers, letters, case, etc).

Key Recovery

The agent interface is used for key recovery purposes. There are two forms of key recovery authorization available in CMS, local and remote. The CISR PKI is currently configured for local authorization.



Local authorization requires the Key Recovery agents to be on the computer hosting the DRM. If the correct passwords are entered, via the agent interface, by the required number of recovery agents, then the DRM retrieves the key and returns the key and its corresponding certificate in a PKCS #12 package. Remote Authorization is initiated by one recovery agent. Once the recovery request is initiated, the DRM sends an email with a specific reference number to all of the other recovery agents. The required number of agents must individually access the DRM's agent interface and using the reference number authorizes the key recovery. The PKCS #12 package containing the key and its certificate are returned to the recovery agent initiating the request. The agent-initiated key recovery process is pictured below.


Data Recovery Manager
Data Recovery Manager agent
HTTPS
Agent Services Key Recovery form
Policy rules
Policy decision
Reject
Logs
Accept
Reject
Key recovery agents
Response form
m of n scheme
Decision
Accept
Internal Database
PKCS #12 package

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arthur Money, "DoD PKI Policy Memorandum," August 12, 2000.

Carlisle Adams and Steve Lloyd, "Understanding PKI, 2nd Edition," Addison Wesley, 2003.

Cryptography World, "The Cryptography Guide," [http://www.cryptographyworld.com/algo.htm], 2003. Accessed June 2004.

Defense Information Systems Agency, "DoD Public Key Infrastructure Introduction," [http://jitc.fhu.disa.mil/pki/intro.html], January 12, 2004. Accessed June 2004.

Department of Defense Public Key Infrastructure Program Management Office, "X.509 Certificate Policy for the United States Department of Defense," December 11, 2003, Version 8.

Digital Signature Trust, "PKI Basics Digital Signatures and Public Key Infrastructure (PKI) 101," [http://wwwdigitalsignaturetrust.com/support/pki_basics.html]. Accessed June 2004.

DoD Chief Information Officer Memorandum, "DoD PKI Milestones Update," October 7, 2003.

DoD Public Key Infrastructure Program Management Office, "PKI Roadmap for the DoD, Version 5.0," December 18, 2000.

Internet Engineering Task Force, "Public-Key Infrastructure (X.509) (pkix)," [http://www.ietf.org/html.charters/pkix-charter.html], May 18, 2004. Accessed June 2004.

Interview via Email between V. Beach, SPAWAR Systems Center and Authors, June 14, 2004.

Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," [http://www.dtic.mil/doctrine/jel/doddict/data/t/05537.html], March 2004. Accessed June 2004.

Microsoft, "Microsoft Windows 2000 Server, Cryptography and PKI Basics," 2000.

Mohan Atreya, "Introduction to PKCS Standards," [http://www.rsasecurity.com/products/bsafe/overview/IntroToPKCSstandards.pdf#xml=http://www.rsasecurity.com/programs/texis.exe/webinator/search/xml.txt?query=pkcs+%2310&pr=default_new&order=r&cq=&id=40c6e13bb], 2004. Accessed June 2004.

National Institute of Standards and Technology, "Introduction to Public Key Technology and the Federal PKI Infrastructure," February 26, 2001.

Netscape Communications Corporation, "Administrator's Guide Netscape Directory Server," [http://enterprise.netscape.com/docs/directory/61/ag/intro.htm#1043886], August 2002. Accessed June 2004.

Netscape Communications Corporation, "Administrator's Guide Netscape Certificate Management System Version 6.1," February 2003. (Administrator's Guide)

Netscape Communications Corporation, "Administrator's Guide, Netscape Security Management System Version 6.1," [http://enterprise.netscape.com/docs/cms/61/cert/pdf/cms61admin.pdf], February 2003. Accessed June 2004.

Netscape Communications Corporation, "Managing Servers with Netscape Console," [http://enterprise.netscape.com/docs/cms/61/admin/ag/1_intro.htm#11284], August 2002. Accessed June 2004.

Netscape Communications Corporation, "Understanding Certificates," [http://developer.netscape.com/docs/manuals/certificate/certagnt/overview.htm], 1997. Accessed June 2004

PKI Forum, "PKI Basics – A Technical Perspective," November 2002.

Ray Hunt, "PKI and Digital Certification Infrastructure," [http://www.au-kbc.org/bpmain1/PKI/PKIieee.pdf], 2002. Accessed June 2004.

Space and Naval Warfare Systems Command Information Systems Security Information Warfare Defense Program Management Office, "Department of Defense Public Key Infrastructure Primer, Version 3.0," 18 June 2001.

The Mozilla Organization, "Using the Certificate Database Tool," [http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html], December 2002. Accessed June 2004.

United States Department of Defense, "Defense Information Infrastructure Certification Authority Certification Practices Statement for Release 3, Version 4.1, May 15, 2002.

United States Department of Defense, "Defense Information Infrastructure Certification Authority Certificate Practices Statement for Class 3 Assurance Version 3.91," August 8, 2001.

Warwick Ford, "A Public Key Infrastructure for U.S. Government Unclassified but Sensitive Applications," September 1, 1995.

Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Transformation Theory 22, pp. 644-654, 1976.

X.509.

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

   LCDR James Downey
   NAVSEA
   Washington, D.C.

7. Richard Hale
   DISA
   Falls Church, Virginia

8. LCDR Scott D. Heller
   SPAWAR
   San Diego, California

9. Wiley Jones
   OSD
   Washington, D.C.

10. Russell Jones
    N641
    Arlington, Virginia

11. David Ladd
Microsoft Corporation
Redmond, Washington

12. Dr. Carl Landwehr
National Science Foundation
Arlington, Virginia

13. Steve LaFountain
NSA
Fort Meade, Maryland

14. Dr. Greg Larson
IDA
Alexandria, Virginia

15. Ray A. Letteer
Head, Information Assurance, HQMC C4 Directorate
Washington, D.C.

16. Penny Lehtola
NSA
Fort Meade, Maryland

17. Ernest Lucier
Federal Aviation Administration
Washington, D.C.

18. CAPT Sheila McCoy
Headquarters U.S. Navy
Arlington, Virginia

19. Dr. Ernest McDuffie
National Science Foundation
Arlington, Virginia

20. Dr. Vic Maconachy
NSA
Fort Meade, Maryland

21. Doug Maughan
Department of Homeland Security
Washington, D.C.

22. Dr. John Monastra
Aerospace Corporation
Chantilly, Virginia

23. John Mildner
SPAWAR
Charleston, South Carolina

24. Marshall Potter
Federal Aviation Administration
Washington, D.C.

25. Dr. Roger R. Schell
Aesec
Pacific Grove, California

26. Keith Schwalm
Good Harbor Consulting, LLC
Washginton, D.C.

27. Dr. Ralph Wachter
ONR
Arlington, Virginia

28. David Wirth
N641
Arlington, Virginia

29. Daniel Wolf
NSA
Fort Meade, Maryland

30. CAPT Robert Zellmann
CNO Staff N614
Arlington, Virginia

31. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, California

32. J. D. Fulp
Naval Postgraduate School
Monterey, California

33. LCDR Vanessa P. Ambers
Naval Postgraduate School
Monterey, California

34. 1LT Amanda M. Kelly
Naval Postgraduate School
Monterey, California