-

NETCOM

Tactics, Techniques, and Procedures (TTP) For Obtaining Soft Certificates for Non-Person Entities

Version 2.1
24 July 2015

This document is not to be distributed or changed without express permission from the Network Enterprise Technology Command (NETCOM). This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom of Information Act. Exemption 5 applies (internal advice, recommendations, and subjective evaluations that are reflected in records pertaining to the decision-making process of or among agencies).

Distribution

This document is intended for use by US Government agencies and their Contractors doing business with the U.S. Army Network Enterprise Technology Command. This document is for information purposes only and is not to be construed as directive in nature or official policy. This document is available by request from NETCOM, ATTN: NETC-G, 2133 Cushing Street, Fort Huachuca, AZ 85613-7070

DISCLAIMER

The contents of this document are not to be construed as an official Department of the Army position unless so designated by other authorized documents. The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to email address: usarmy.huachuca.netcom-9-sig-cmd.mbx.eeupdate@mail.mil.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

X

GERALD H MILLER
COL, GS

DOCUMENT REVISIONS LIST

DATE	DESCRIPTION OF CHANGES	ORGANIZATION
16 Dec 12	Initial document	NETCOM, G5
12 Jun 12	Updated email address and changed to Version 1.1	NETCOM, G5
24 Sep 13	Converted to current template format	NETCOM, G3
13 Dec 13	Final formatting	NETCOM, G3
30 May 14	Annual format review.	NETCOM, G34
12 Dec 14	Process update, clarification, and correction	ARCYBER and PO EE
2 Mar 15	Clarification on exporting public keys	PO EE
1 May 15	Finalization of details for authentication certificates	PO EE, CIO/G-6
23 Jul 15	Clarification on submitting ticket to DISA	PO EE

TABLE OF CONTENTS

1.0 Purpose 1
2.0 References 1
3.0 Scope 1
4.0 Procedures 1
4.1 Request Certificates for NPE Mailboxes 1
4.2 RA Issues Certificates.....2
4.3 Save Public Key to a .CER File.....3
4.4 Have DISA associate certs with NPE.....3
4.5 Validate functionality 4
4.6 New Users 4
4.7 Change of Users 4
4.8 Custodianship 4
Appendix A: Acronyms 1
Appendix B: Sample Memo 1

TABLE OF FIGURES

Figure 1: Sample DA Request Memorandum 1

EXECUTIVE SUMMARY

In accordance with Department of Defense (DoD) Directive 8500.1, NETCOM will implement equipment certificates for every Non-Personal Entity (NPE) to bolster security through the enterprise. NPEs for organizational and/or group accounts are required to obtain soft certificates from the Defense Information System Agency (DISA) Certificate Authority (CA) in order to operate on the Army enterprise network. As defined in this document, NPEs pertain to DoD Enterprise Email (DEE) mailboxes. The soft certificates are delivered via files that contain certificates. These files are requested by Public Key Infrastructure (PKI)-NPE Trusted Agents (TA). This document covers the Registration Authority (RA) and other components.

1.0 Purpose

This document has been developed to explain, in detail, the process of requesting soft certificates for NPEs to be used in the DEE system.

2.0 References

Army PKI Phase 2 Implementation Instructions Version 2.5.

3.0 Scope

This document provides the prescribed procedures to be followed by system administrators for procurement and attachment of PKI certificates to organizational or group NPE mailboxes within the DEE environment.

4.0 Procedures

Use the process below to enable an NPE mailbox to send signed email (using a signing certificate) and receive encrypted mail (using an encryption certificate). It is also used to allow a mobile device or automated process to authenticate and access an NPE mailbox (using an authentication certificate).

4.1 Submit a request for NPE Mailbox certificates

a. The local commander, minimum rank of GS-15/O-6, of the group wishing to obtain certificates for NPE mailboxes will submit a signed “Request Memorandum” to the Army Registration Authority mailbox, USARMY Pentagon HQDA CIO G6 Mailbox Army Registration Authority, (usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil). Upon request, the RA can provide a sample memorandum. See Appendix B for a sample memo.

b. The “Request Memorandum” requires the following information.

1) The local Information System Security Officer (ISSO) must coordinate with their Trusted Agent (TA). The TA must submit the request because the TA will receive the files in return. The request must include the name, email address, and phone number of the ISSO.

2) The name and office symbol of the organization using the group certificates.

3) The name, email address, and phone number of all persons who will use the certificates.

4) Identify who will be the primary custodian and one (1) or two (2) alternate custodians. The primary custodian may be the ISSO, but is not required to be.

5) The display name and email address of the NPE to which the certificates will be bound.

6) The certificates required. (Determine what actions you will perform with the NPE Mailbox to determine the certificates required: sign only, sign and encrypt/decrypt, authenticate using a mobile device or automated process).

a) If only signing, then simply request a signature certificate.

b) If signing and encrypting/decrypting, then request **both** a signature certificate and an encryption certificate.

c) If an authentication certificate is required, this MUST be clearly identified in the request by an additional statement indicating that a certificate to be used for authentication is required.

7) If the organization requires certificates for more than one NPE, the requests may be on a single request memo but must clearly indicate which personnel will have access to which certificates.

c. Submit a signed DD Form 2842 for each person using the certificates

Each person accessing the group certificates must sign a Department of Defense (DD) Form 2842 acknowledging their responsibilities. If the individuals are located at a site remote from the Army RA Office, the DD Form 2842s will be submitted to an approved TA who will verify the person's identity and mail the forms to the Army RA office at the address shown below. The TA may scan the forms and email them by encrypted email to usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil to facilitate Certificate Registration Instructions (CRI) issuance. Original documents must be mailed later to the following address:

Army Registration Authority
5850 23rd Street
Building 220
Fort Belvoir, VA 22060

d. Upon receipt of the "Request Memorandum" and signed DD Form 2842s for each person accessing the certificates, the Army RA will consider the validity of the request.

4.2 RA Issues Certificates

a. If the request is considered to be valid and is only for signature and/or encryption certificates, the Army RA will issue a CRI to the TA. (If the request is not valid, the Army RA will return the request to the requesting organization.) The TA will deliver the CRI to the ISSO/primary custodian who will download the certificates to a Compact Disk - Read Only Memory (CD-ROM) disk. The TA will ensure that each person listed on the group memo will complete the DoD "Acknowledgement of Responsibilities Form" and email the digitally signed forms back to the Army Registration Authority mailbox (usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil).

b. If the request is considered to be valid and is for an authentication certificate (either with or without the other certs), the Army RA will issue the .p12 or .pfx files to the TA and will send the password for the certs to the primary custodian or alternate custodian. (The point is that certificates will be sent to one person and the password to another person on the memo.) The reason for this alternate method is because the Army RA must download and then use the ID cert to create the authentication certificate.

c. The ISSO/primary custodian will install the certificates in the computer profile/account for each user/application authorized to use the certificates. Installing certificates on the computer is accomplished by double-clicking the .p12 (or .pfx) file(s) and walking through the certificate import wizard. The certificates will only be installed as "non-exportable" to ensure rogue copies of the certificates cannot be created.

d. The ISSO/primary custodian will store the primary certificates on CD-ROM disk in a locked container within the office. The corresponding password (allowing use/access of the certificate, much like a user's CAC PIN) will be secured separately also in a locked container.

4.3 Export the Public Key to a .CER File. Use the following steps to export the public key information to a certificate file. The only certificates to be exported are the one (or two) that will be provided to DISA.

a. Open the “Certificates Console”.

1) Select the Start button to get the search field.

2) Type “MMC” and press “Enter”.

3) When the console opens, select “File” then “Add/Remove Snap-in”.

4) Select “Certificates” in the left column and click “Add” (to put it in the right column).

5) Click “OK”.

b. Navigate to the correct certificate folder in the left column. This is normally done by clicking the arrow next to “Certificates – Current User”, then the arrow next to “Personal”, then clicking the “Certificates” folder, and then selecting the correct certificate (for the NPE) in the center column.

c. Once you have selected the cert in the center column, the cert name should appear in the lower bar of the right column (Actions) with a “More Actions” drop down menu beneath it. Click the “More Actions” and select “All Tasks – Export” and the Certificate Export Wizard should appear. Click “Next”.

d. Leave the selection as “No, do not export the private key” and click “Next”.

e. Leave it as a “DER encoded binary X.509 (CER)”, click “Next” and then save the file and click “Finish”. Name the file with the NPE display name and underscores where there are spaces in the name (ex: DoD_EE_NPE_Display_Name.cer).

f. Once the one or two certificates are exported, close the management console.

4.4 Open a trouble ticket to DISA and have DISA associate certs with NPE

a. Once the certificate has been exported, open a ticket with the service desk through the standard ticketing process (requesting the ticket be escalated to DISA). The ticket will require the following information in addition to the standard required information.

1) DEE NPE display name.

2) DEE NPE email address.

3) Attach the public key of the NPE Encryption certificate (the binary encoded .cer file you just exported in 4.3 above) to the ticket. Because Outlook won’t transfer .cer files, you must rename the .cer file with a “.txt” extension, and indicate that the attached .txt file is really a .cer file and must be re-named.

4) If the NPE must be viewed on a BB10 or an automated process/application will use the NPE to send email, request that the NPE be “Enabled for interactive login”, and also attach the NPE authentication certificate to the ticket (as a .txt file).

5) If the NPE must be viewed on a BB10, also request that the BlackBerry Entitlement be added to the NPE account.

b. The service desk will escalate the ticket to DISA’s DEE service desk for association of the certificates with the DEE NPE.

c. Once the certificate is associated with the NPE, the DEE service desk will provide a response and the update will be communicated back to the end-user through the established service desk process.

4.5 Validate functionality

a. The user should send a test email from the NPE mailbox signing it with the new signing soft certificate associated with the NPE.

b. If an encryption cert was requested, the end-user should also test encryption to the new NPE.

c. If an automated process will use the NPE, the ability to authenticate to the NPE using the certificate should be tested by using webmail and selected the NPE Authentication certificate to authenticate. (Go to https://web.mail.mil and after clicking “OK” the NPE certificate should come up as an option along with the user’s personal certificates. Ensure you select the authentication certificate.)

d. If the user must view the NPE on a BB, the user must check their BB to ensure they can view the mailbox.

e. The end user will then provide a response indicating if the certificate was able to be utilized correctly to allow the ticket to be closed or the end-user will provide feedback if issues exist.

4.6 New Users

If new users (not originally listed on the group certificate memo) are added to the NPE mailbox and need to use the certificates, a DD Form 2842 must be signed and submitted to the Army RA Office.

4.7 Change of Users

If a user is removed from being able to use the mailbox, a new certificate password must be generated. The primary custodian must request a new certificate password through the Army Registration Authority by sending a new signed memo (with the new list of users) to the Army Registration Authority mailbox identifying the org mailbox and the certificate that needs a new password (using the information from the original memo).

4.8 Custodianship

In the event the primary custodianship changes, the outgoing custodian will sign the disk over to the new custodian. The new custodian will follow the procedures listed in this TTP. The new custodian will change the certificate key password.

Appendix A: Acronyms

ACL	Access Control List
CA	Certificate Authority
CD-ROM	Compact Disk-Read Only Memory
CRI	Certificate Registration Instructions
DD	Department of Defense
DEE	Department of Defense Enterprise Email
DISA	Defense Information Services Agency
DoD	Department of Defense
ISSO	Information Systems Security Officer
NETCOM	Network Enterprise Technology Command
NPE	Non-Person Entity
NUN	NPE User Name
PKI	Public Key Infrastructure
RA	Registration Authority
TA	Trusted Agent
TTP	Tactics, Techniques, and Procedures
UPN	User Principal Name

Appendix B: Sample Memo

DEPARTMENT OF THE ARMY
ENTER UNIT INFO HERE
ENTER ADDITIONAL UNIT INFO HERE
ENTER STREET ADDRESS HERE
FORT ENTER, HERE, 00000

REPLY TO
ATTENTION OF

Sample Memorandum. Items in Italics are to be changed to reflect the requesting organization's information.

Enter Office Symbol HERE → → → → → → *Enter Date HERE*

MEMORANDUM FOR US ARMY REGISTRATION OFFICE, 5855 21st Street, Bldg 215, Fort Belvoir, VA 22060

SUBJECT: → Request for Group PKI Certificates

1. The _*Insert Office Name*_____Office requests issue of group PKI certificates for our organizational mailbox: _____.

2. The following is a list of the users who will have access to these certificates. Each of these users has completed a DD Form 2842, accepting their responsibilities in protecting these certificates.

   a. *CPT John Smith, john.a.smith.mil@mail.mil, phone: (999) 999-9999, ISSO/Primary Custodian*
   b. *1LT Mary Jones, mary.b.jones.mil@mail.mil, IMO, phone: (999) 999-9998, Alternate Custodian*
   c. *SFC Bobby Joe Green, bobby.j.green.mil@mail.mil, phone: (999) 999-9997,*

3. The NPE for which the certificates are required is: *USARMY Fort X Sub-org Y Mailbox Description, usarmy.x.sub-org-y.mbx.description@mail.mil*

4. Both a signing certificate and an encryption certificate are required.

5. The ISSO/Primary Custodian will maintain the primary certificates, on disk, in a secure location within the office. The corresponding password will be secured separately, also in a locked container. An Access Control List (ACL) will be maintained near the computer or computers on which the group certificate is used.

6. Upon reassignment of any user on the ACL, the ISSO/Primary custodian will either remove the group certificates from the user's workstation or reinstall the certificates from the floppy with a new password.

7. In the event primary custodianship changes, the outgoing custodian will sign the disk over to the new custodian. The new custodian will follow the procedures listed in paragraph 4 (above) and change passwords accordingly.

6. Point of contact for this request is *CPT John Smith at (999) 999-9999 or john.a.smith.mil@mail.mil.*

→ → → → → → → *GEOFF W. BROWN*
→ → → → → → → *COL, GS*
→ → → → → → → *(Commander,*
→ → → → → → → *Security Manager,*
→ → → → → → → *GS 15 or higher)*

Figure 1: Sample DA Request Memorandum