Utilizing the DoD PKI to Provide Certificates for Unified Capabilities (UC) Components

DISA NS2 Capabilities Center
November 3, 2011
Revision 1.2

Change Table

Change	Date	Author
• Removed references to "RTS" and replaced with "UC" • Changed OCSP responder sections to reflect that ocsp-legacy.disa.mil URL was deactivated on Nov 1, 2010. Only OCSP DTM is now supported • Added IP addresses of OCSP responders corresponding to ocsp.disa.mil URL • Added instructions for verifying CSRs using OpenSSL • Added an example action item register for all DoD PKI related activities • Inserted warnings to backup the private keys associated with a CSR	November 19, 2010	DISA NS2 Team
• Noted that 2048 bit certificates are now the only ones that can be ordered from the NIPRNET DoD PKI CAs • Corrected the steps for retrieving ordered certificates from the CA websites and updated screenshots • Added additional IP addresses for OCSP responders and CRL distribution points • Added DISA RA Operations contact information for CSRs submitted to DISA • Added information on OCONUS OCSP URLs • Added a more detailed diagram illustrating the OCSP delegated trust model (DTM) • Added new section, 2.11, which describes the information that must be added to an IT helpdesk ticket to open up firewalls and web proxies for OCSP and CRL requests/responses	March 17, 2011	DISA NS2 Team
• Updated IP addresses associated with the crl.disa.mil and crl.gds.disa.mil CRL distribution points	September 7, 2011	DISA NS2 Team
• Updated to address new CAs coming online in December 2011 (CA-27, CA-28, CA-29, and CA-30), new static CRL URLs , and CRIMSON tool availability	November 2, 2011	DISA NS2 Team

Table of Contents

1 Ordering Certificates from the DoD PKI 5
1.1 Contacting Your Local Registration Authority to Expedite Service 5
1.2 Generating a Certificate Signing Request (CSR) 6
1.2.1 What Information is Required to Generate a Signing Request? 6
1.2.2 Using Commercial Tools or UC Equipment to Generate a CSR 8
1.2.3 How many certificates do I need to request? 9
1.3 Uploading the Request to the DoD PKI Certificate Authority 10
1.3.1 Use of One DoD PKI Certification Authority Versus Another 10
1.3.2 Websites Used to Upload Certificate Signing Requests 10
1.3.3 Selecting the Certificate Profile 11
1.3.4 Uploading the PKCS#10 Certificate Signing Request 12
1.3.5 Adding Additional Identities to the Certificate 13
1.3.6 Inputting the Requester’s Contact Information 14
1.3.7 Confirmation of Your Submitted Request 14
1.3.8 Checking the Status of a Submitted Certificate Request 15
1.4 Submitting the Certificate Request to a Local Registration Authority 15
1.4.1 Tips for Expediting Your Certificate Request 15
1.4.2 Submitting the Certificate Request to the Air Force LRA 16
1.4.3 Submitting the Certificate Request to the Army LRA 16
1.4.4 Submitting the Certificate Request to the Navy LRA 17
1.4.5 Submitting the Certificate Request to the US Marine Corp LRA 17
1.4.6 Submitting the Certificate Request to the DISA Registration Authority 17
1.4.7 Submitting the Certificate Request for All Other Organizations 17
1.5 Loading the Trust Chains and CRL/OCSP Pointers into Equipment 18
1.5.1 Loading DoD PKI Trust Chains 18
1.5.2 Configuration of CRLs and OCSP Responders 18
1.6 Retrieving and Loading Your DoD PKI CA Issued Certificate 20

2 Other Frequently Asked Questions 22
2.1 How can I contact the DoD PKI PMO to obtain assistance? 23

2.2 Certificate Revocation Lists (CRLs) 23
2.2.1 What is a Certificate Revocation List? 23
2.2.2 How can I obtain a Certificate Revocation List from the DoD PKI? 23
2.2.3 What If I Need an IP Address for the CRL Distribution Point? 24
2.2.4 Should I Use HTTP or LDAP to Retrieve CRLs? 25
2.2.5 How Often Should CRLs Be Retrieved? 25
2.3 Online Certificate Status Protocol (OCSP) 25
2.3.1 What is OCSP? 25
2.3.2 What is an OCSP Responder? 26
2.3.3 What is the OCSP Delegated Trust Model (DTM)? 26
2.3.4 What are the URLs for the DoD PKI's OCSP Responders? 29
2.3.5 What if I need an IP address for the OCSP Responder instead of a URL? 29
2.3.6 How can I obtain the self-signed certificate for the legacy OCSP responders? 30
2.3.7 Why do the OCSP Responders use HTTP instead of HTTPS? 30
2.4 Which is better: OCSP or CRLs? 30
2.5 Maintaining Valid DoD PKI Certificates in UC Equipment 30
2.5.1 How Often Do DoD PKI Certificates Need to Be Replaced? 30
2.6 Should I Order 2048 Bit Certificates or 1024 Bit Certificates? 31
2.7 Where Can I Obtain All of the DoD PKI Certificate Authority Certificates? 31
2.8 What if I Only Need Test Certificates? 32
2.8.1 Website for Submitting Certificate Requests to JITC 32
2.8.2 Submitting the Test Certificate Request to Your LRA 32
2.8.3 Downloading Test Trust Chains 32
2.8.4 JITC OCSP Responder 33
2.8.5 Points of Contact to Obtain Assistance with JITC Test Certificates 33
2.9 How Can I View Certificate Data Using the Windows Certificate Viewer? 33
2.10 How Can I Use OpenSSL To Validate and View Certificate Signing Requests? 34
2.11 What Do I Need to Tell My IT Staff to Allow Through Our Firewall? 34
2.12 Is There a Way To Request Certificates in Bulk? 35

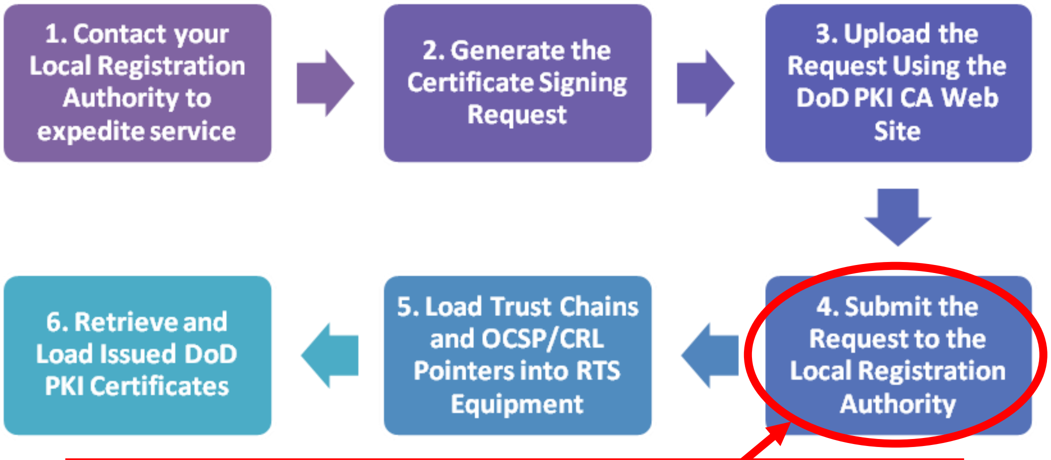
3 Acronyms 36

Appendix A: Troubleshooting Tips 38

Appendix B: Example DoD PKI Action Item Register 39

1 Ordering Certificates from the DoD PKI

Unified Capabilities (UC) equipment, including devices like Softswitches (SS), Local Session Controllers (LSC), End Instruments (EIs), and Edge Boundary Controllers (EBC) require the use of X.509 certificates to provide confidentiality and establish mutually authenticated secure connections for telecommunications sessions. The Department of Defense Public Key Infrastructure (DoD PKI), operated by the Defense Information Systems Agency (DISA), is expected to be the primary source for these certificates. In order to successfully operate UC components using the DoD PKI, administrators must execute the following five steps:


1. Contact your Local Registration Authority to expedite service
2. Generate the Certificate Signing Request
3. Upload the Request Using the DoD PKI CA Web Site
4. Submit the Request to the Local Registration Authority
5. Load Trust Chains and OCSP/CRL Pointers into RTS Equipment
6. Retrieve and Load Issued DoD PKI Certificates

This step has the potential to cause the most delay. Please review Sections 1.1 and 1.4.1 for more information on expediting this step.

This guide is primarily designed to assist DoD personnel and hired technicians with obtaining operational, DoD PKI issued, certificates for use in UC devices. This guide should not be used by those seeking to obtain DoD PKI issued certificates or tokens for human identification purposes (such as Common Access Cards), since this process will differ. Also, for those who only need test (non-operational) DoD PKI certificates, this information is located in Section 2.8.

The six steps shown above illustrate the process for obtaining DoD PKI certificates at a high level. A more detailed action item register has been added to Section 0 of this guide to assist UC site program managers with tracking all of the critical DoD PKI enablement actions.

1.1 Contacting Your Local Registration Authority to Expedite Service

Technicians in the field requesting certificates for UC equipment have reported delays of several days or more AFTER uploading the certificate request to the DoD PKI CA website. This delay stems from the time it takes the Local Registration Authority (LRA) to approve the certificate request. The LRA is the primary "human element" involved in the approval process and all certificate requests must go through your resident LRA. In order to expedite your certificate request(s), it is recommended that you call your LRA early in the process, prior to submitting the certificate request(s), to find out if any options exist for expediting certificate generation service. This call will help to acquaint you with the LRA and help you to understand the submission process. Also, this call will provide early notice for the LRA so that they become aware of your pending request and make the appropriate preparations. Note that many LRAs require additional forms to be submitted before they approve the certificate request. Therefore, it is recommended that certificate requesters fill out any such forms and return them as quickly as possible to avoid delays with certificate delivery. Request these forms along with example, pre-filled forms or templates during your initial call to the LRA. It is recommended that this occur as the first step, rather than waiting until Step #4, where the LRA is contacted after the certificate signing request has been uploaded. Section 1.4 contains the procedures for contacting your LRA.

1.2 Generating a Certificate Signing Request (CSR)

1.2.1 What Information is Required to Generate a Signing Request?

When a UC component communicates with a remote device, the remote device requires authentication before permitting access to its services. In this case, the UC component must present a set of credentials, which can be verified by the remote device, in order to prove its identity. In other cases, the UC component may need to establish a shared secret with a remote device so that no other entities on the network can eavesdrop on the communication. Certificate Authorities (CAs) make these scenarios possible by using cryptographic techniques to “digitally sign” a set of credentials, which can then be used for the purposes of identification and confidentiality. The CA must be trusted by both communicating parties in order to allow this trusted exchange of cryptographic information to occur.

In order for the DoD PKI CA to create a certificate, it has to know what information to “digitally sign.” When providing certificates for a human, this set of information would include things like the person’s name and the organization to which they belong. But for a device, like an Edge Boundary Controller (EBC), this information would include things like an IP address or the Fully Qualified Domain Name (FQDN) assigned to the device. The use of a FQDN is preferred.

The following table summarizes the information that will minimally need to be known for each interface on the device that requires certificates in order to generate the “Certificate Signing Request” (CSR), also known as the “to-be-signed certificate:”

<table>
<tr><th colspan="4">Information Required to Create a Certificate Signing Request for an UC Device</th></tr>
<tr><th>Field</th><th>Example</th><th colspan="2">Notes</th></tr>
<tr><td>Name</td><td>ebc1red</td><td colspan="2">A unique name for interface on the UC component to which this certificate will be assigned</td></tr>
<tr><td>Country (C)</td><td>US</td><td>The country associated with the entity controlling this equipment. This will generally be “U.S.” for the DoD PKI (External Certificate Authorities, which use a separate root from the DoD PKI, can grant certificates for foreign nationals)</td><td rowspan="5">NOTE:
The Local Registration Authority may edit these fields after the CSR has been submitted. (See Section 1.4)</td></tr>
<tr><td>State (ST)</td><td>Texas
(this field is not always used)</td><td>The state associated with the entity controlling this equipment.</td></tr>
<tr><td>Locality (L)</td><td>Lackland AFB
(this field is not always used)</td><td>The locality associated with the entity controlling this equipment.</td></tr>
<tr><td>Organization (O)</td><td>U.S. Government</td><td>The organization associated with the entity controlling this equipment.</td></tr>
<tr><td>Unit (OU)</td><td>DoD
(this field may appear multiple times, example: OU=DoD, OU=PKI, etc.)</td><td>Enter the unit associated with the entity controlling this equipment.</td></tr>
<tr><td>Common Name (CN) (populates the Common Name value in the Certificate’s “Subject” field)</td><td>server1.example.dod.mil
or
192.168.2.100
(depending on whether an FQDN or IP address is used – FQDN is preferred for this field)</td><td colspan="2">The IP (v4 or v6) address or Fully Qualified Domain Name (FQDN) assigned to this device (use of a fully qualified domain name is recommended because IP addresses can change as the network is redesigned or moves from IPv4 to IPv6, necessitating reissuance of certificates. Also recent guidance from the JITC PKI lab suggests that IP addresses may not be allowed in the future.)
The naming conventions in DISA NS2 published UC deployment guides should be followed.</td></tr>
<tr><td>Key Size
(2048 bits, may differ for SIPRNET)</td><td>2048</td><td colspan="2">It is recommended that the 2048 bit size be used wherever possible given its greater security strength. The DoD PKI has ceased issuance of 1024 bit certificates on NIPRNET as of the end of 2010. See Section 2.6 for details.</td></tr>
</table>

The Department of Defense (DoD) requires the Common Name (CN) identified in the certificate be unique across the entire DoD. The easiest way to ensure uniqueness is to use a Fully Qualified Domain Name (FQDN). Current DoD PKI specifications indicate that Internet Protocol (IP) addresses can also be used, but these can be volatile as networks are consolidated and redesigned.

Note that if FQDNs are used, you may need to configure your Domain Name Service (DNS) servers to map these FQDNs to IP addresses or manually configure name resolution tables locally on the device so that the FQDN placed in the certificate and assigned to the equipment resolves to the appropriate IP address. This step is not necessary for all applications that use certificates (e.g. management interface may require this, but the call signaling interface may not) so be sure to check with the vendor of your equipment to determine whether this step is required. Also, check with your UC equipment vendor to ensure that it supports the use of FQDNs in certificates.

1.2.2 Using Commercial Tools or UC Equipment to Generate a CSR

Some UC devices can generate their own certificate signing request while other devices rely on the use of commercial tools to generate the signing request. The request is generated by taking the information identified in Section 1.2.1 and creating a standard formatted message called Public Key Cryptography Standard (PKCS) #10 message. Other certificate signing request formats exist, however PKCS#10 is the format primarily used with the DoD PKI and supported by most equipment.

If your equipment does not support generation of a certificate signing request, the Air Force has developed a detailed guide explaining how to generate a certificate signing request using the information identified in Section 1.2.1 and it is located at the following website:

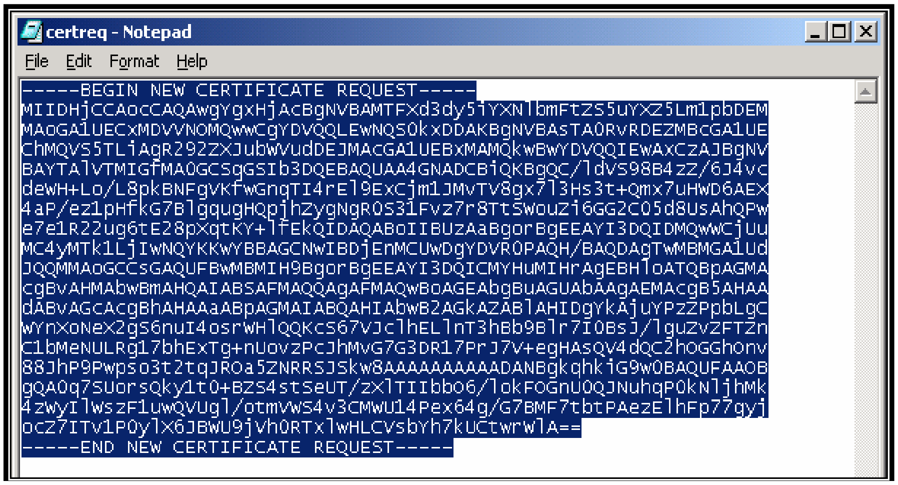
https://afpki.lackland.af.mil/html/pke_cots.asp (this site is accessible from .mil domains only)

This website provides step-by-step guidance on generating a certificate request using many standard commercial products. The DoD PKI is also in the process of developing a tool called CRIMSON which will assist with this aspect of the process, however this tool will not be available until mid-CY 2011. A beta version is available for download by visiting www.forge.mil.

Ensure that you are using a NIST FIPS 140-2 validated product to generate your certificate signing request and public/private RSA key pairs. Use of FIPS 140-2 validated cryptography ensures that cryptographic operations, such as generating key pairs, are being correctly performed and use strong randomization. Also, if the equipment itself did not generate the key pairs and signing request, take the appropriate precautions to secure the private key associated with the certificate signing request. Especially since the private key will eventually need to be loaded into the UC component. Most tools will provide an option to use a password to protect the private key so that it is not stored in plaintext format.

Create a backup copy of the private key corresponding to a certificate signing request and store it in a secured location. If one loses the private key corresponding to the CSR, then the certificate returned from the DoD PKI cannot be used. In fact, the DoD PKI will have to revoke the certificate, which increases the size of the DoD PKI CA's certificate revocation list, increases the bandwidth used to perform revocation checking, and increases operational costs. The DoD PKI LRAs also may require remedial training and a review of site procedures if private keys are lost. For these reasons, take precautions to ensure that the private key is adequately safeguarded.

The end result of this step is that you will have generated a PKCS#10 file or message that resembles the following. Save this information for use later when the request is submitted to the appropriate Certificate Authority.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDHjCCAocCAQAwgYgxHjAcBgNVBAMTFXd3dy5iYXNlbmFtZS5uYXZ5Lm1pbDEM
MAoGA1UECxMDVVNOMQwwCgYDVQQLEwNQS0kxDDAKBgNVBAsTA0RvRDEZMBcGA1UE
ChMQVS5TLiAgR292ZXJubWVudDEJMAcGA1UEBxMAMQkwBwYDVQQIEwAxCzAJBgNV
BAYTAlVTMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/ldvS98B4zZ/6J4vc
deWH+Lo/L8pkBNFgVKfwGnqTI4rEl9ExCjm1JMvTV8gx7l3Hs3t+Qmx7uHWD6AEX
4aP/ez1pHfkG7BlgqugHQpjhZygNgR0S31Fvz7r8TtSwouZi6GG2C05d8UsAhQPw
e7e1R22ug6tE28pXqtKY+lfEkQIDAQABoIIBUzAaBgorBgEEAYI3DQIDMQwWCjUu
MC4yMTk1LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYDVR0PAQH/BAQDAgTwMBMGA1Ud
JQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMA
cgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAA
dABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDgYkAjuYPzZPpbLgC
wYnXoNeX2gS6nuI4osrWHlQQKcS67VJclhELlnT3hBb9Blr7I0BsJ/lguzvzFTZn
C1bMeNULRg17bhExTg+nUovzPcJhMvG7G3DR17PrJ7V+egHAsQV4dQC2hoGGhonv
88JhP9Pwpso3t2tqJROa5ZNRRSJSkw8AAAAAAAAAADANBgkqhkiG9w0BAQUFAAOB
gQA0q7SUorsQky1t0+BZS4stSeUT/zXlTIIbbo6/lokFOGnU0QJNuhqP0kNljhMk
4zwyIlwszF1uwQVUgl/otmVwS4v3CMWU14Pex64g/G7BMF7tbtPAezElhFp77gyj
ocZ7ITv1P0ylX6JBWU9jVh0RTxlwHLCVsbYh7kUCtwrWlA==
-----END NEW CERTIFICATE REQUEST-----
```

Note that the "-----BEGIN NEW CERTIFICATE REQUEST-----" and the "-----END NEW CERTIFICATE REQUEST-----" lines are part of the PKCS#10 message and should be included when cutting and pasting this certificate signing request.

1.2.3 How many certificates do I need to request?

The number of certificates that need to be ordered will depend on the following:

1.) The number of Multifunction Softswitch (MFSS) servers comprising the MFSS configuration, Local Session Controller servers, and Edge Boundary Controllers (EBCs, either a single EBC or high availability dual-EBC configuration) that will be deployed at the site. As an example, the number of certificates required for a recently installed MFSS was 9. On the other hand, the single EBC and High Availability EBC solution require two certificates (one for the interface internal to the enclave and one for the interface external to the enclave).

2.) The number and type of interfaces the device supports which require certificates (Example 1: a device that supports use of a DoD PKI certificate for SSL/TLS web-based management and a second certificate used to communicate call signaling messages to other UC devices. Example 2: a device that requires a certificate to establish an IPSec tunnel and a second certificate to secure call signaling messages using TLS).

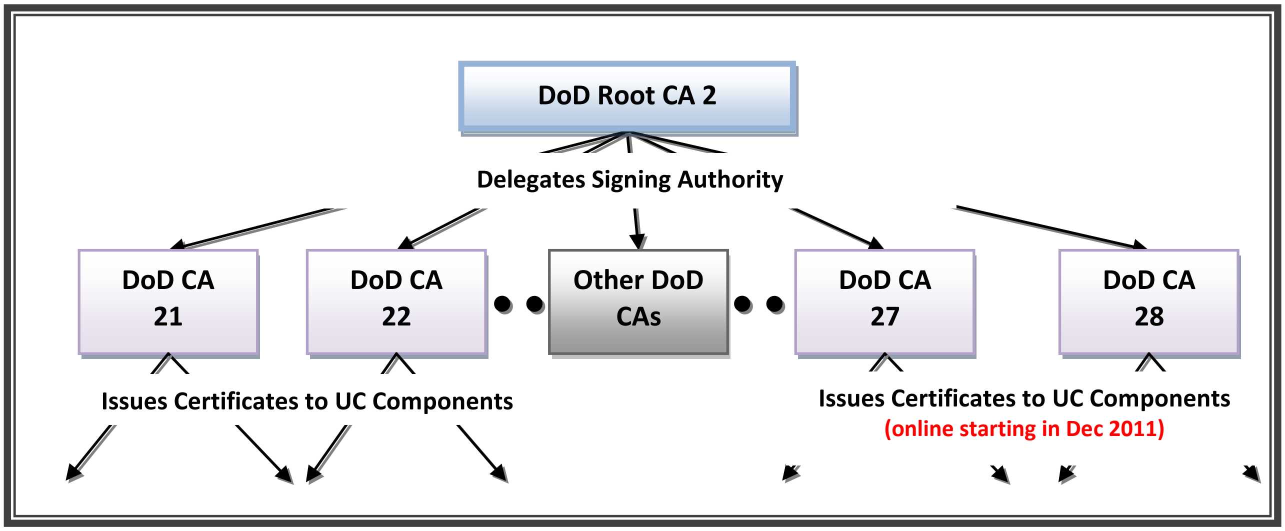
3.) The number of remote ancillary equipment (RAE) systems, like RADIUS servers, Syslog servers, etc., that utilize DoD PKI certificates

4.) The number of security devices like Firewalls, Virtual Private Network servers, and Intrusion Detection Systems that utilize DoD PKI certificates on any of their interfaces

You can check with the vendor of your equipment to determine exactly how many certificates are required.

1.3 Uploading the Request to the DoD PKI Certificate Authority

Once the request is generated, you can submit the request to the DoD PKI Certificate authority. The DoD PKI does not have a single certificate authority that issues/signs certificates. Instead, the DoD PKI is currently (as of the writing of this document) structured in a hierarchical manner as shown:


DoD Root CA 2
Delegates Signing Authority
DoD CA 21
DoD CA 22
Other DoD CAs
DoD CA 27
DoD CA 28
Issues Certificates to UC Components
Issues Certificates to UC Components
(online starting in Dec 2011)

Due to the hierarchical nature of the DoD PKI, when configuring equipment, the best results may be obtained by first loading the DoD PKI Root, followed by intermediate CAs (like CA-21 and CA-22 or CA-27 and CA-28), and lastly loading other certificates. See Section 1.5.1 for more information. Also, note that each CA in the hierarchy publishes its own certificate revocation list (CRL) for the certificates that it directly issues. See Section 1.5.2 for additional detail.

1.3.1 Use of One DoD PKI Certification Authority Versus Another

At the time of this document's writing, either DoD PKI CA-21 or DoD PKI CA-22 can be used to obtain certificates. However, be sure to check with DoD PKI help desk to find out the latest information on the appropriate CA to use because these CAs are continually updated and replaced. For example, starting in December 2011, components will be able to use CA-27 and CA-28 to obtain device certificates for UC devices. Typically components should use the newest CAs to obtain device certificates in order to ensure that they can obtain certificates with the maximum expiration time.

1.3.2 Websites Used to Upload Certificate Signing Requests

The following websites can be used to submit the certificate signing request generated in Section 1.1:

Certificate Signing Request Upload Websites (On NIPRNET)	
Website for CA-21	https://ca-21.c3pki.chamb.disa.mil/ (Caution: This URL may migrate to *.csd.disa.mil without notice)
Website for CA-22	https://ca-22.csd.disa.mil/
Load Balanced DoD PKI CA (Directs your request to either CA-21 or CA-22)	https://id-sw.csd.disa.mil/
Website for CA-27	TBD – Not online until December 2011
Website for CA-28	TBD – Not online until December 2011

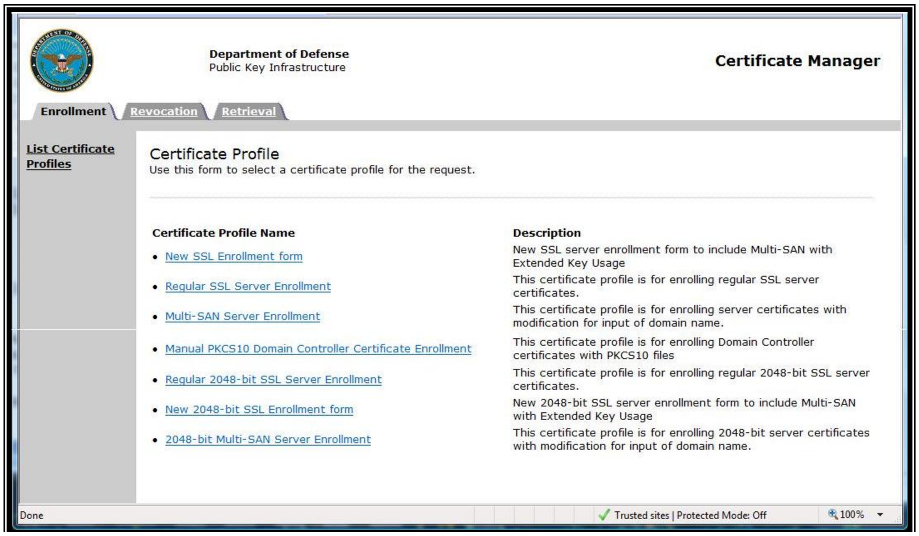
SIPRNET certificate requests must be submitted on SIPRNET. Replace .mil with .smil.mil in the URLs above. All other processing described in the following sections should be the same.

A CAC or DoD PKI soft certificate is not required in order to log onto these websites, however you should have the DoD PKI roots installed into your web browser in order to avoid any website security warnings from your browser. You can obtain the DoD PKI roots for loading into your browser by following the instructions in Section 2.7.

Note that these websites and the following instructions in this section are for obtaining operational DoD PKI certificates. If you need test certificates, please see Section 2.8.

1.3.3 Selecting the Certificate Profile

Once you have logged into the DoD PKI CA, you should see a screen like the following:



Certificate Profile

Use this form to select a certificate profile for the request.

Certificate Profile Name	Description
New SSL Enrollment form	New SSL server enrollment form to include Multi-SAN with Extended Key Usage
Regular SSL Server Enrollment	This certificate profile is for enrolling regular SSL server certificates.
Multi-SAN Server Enrollment	This certificate profile is for enrolling server certificates with modification for input of domain name.
Manual PKCS10 Domain Controller Certificate Enrollment	This certificate profile is for enrolling Domain Controller certificates with PKCS10 files
Regular 2048-bit SSL Server Enrollment	This certificate profile is for enrolling regular 2048-bit SSL server certificates.
New 2048-bit SSL Enrollment form	New 2048-bit SSL server enrollment form to include Multi-SAN with Extended Key Usage
2048-bit Multi-SAN Server Enrollment	This certificate profile is for enrolling 2048-bit server certificates with modification for input of domain name.

On this page, you will see a number of certificate profiles presented. It is recommended that administrators use the following profile:

Recommended DoD PKI Certificates Profiles to Use with UC Equipment		
Certificate Profile Name	**Key Size**	**Description**
New 2048-bit SSL Enrollment Form	2048	Same as the "New SSL Enrollment Form" profile except that the 2048 bit key size is used. Use of this profile over the 1024 key size version is recommended.[1]

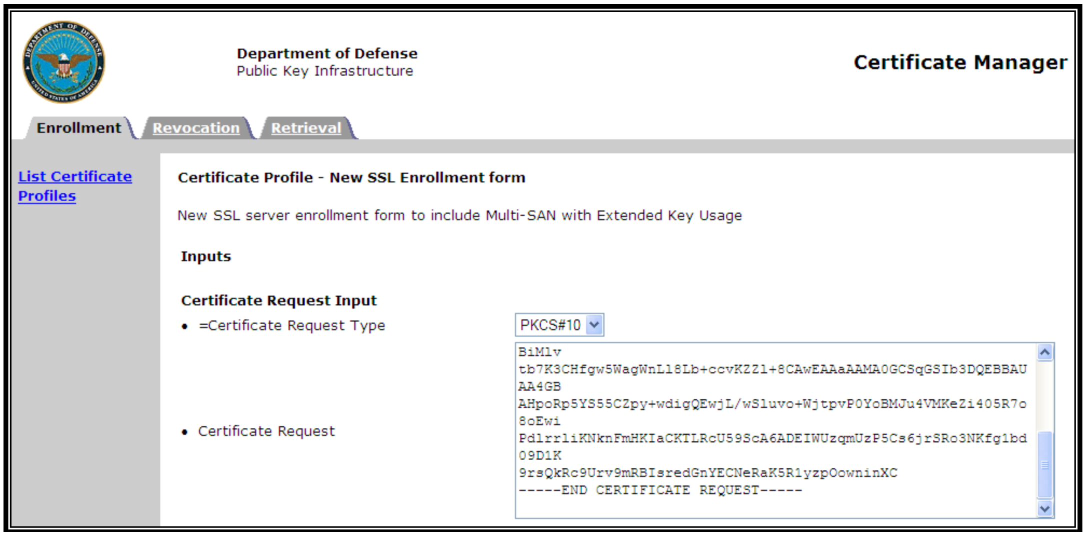
[1] For any issues encountered while submitting requests using these profiles, troubleshooting tips can be found in Appendix A.

Other profiles should only be used if there is a specific reason to do so. For example, the equipment vendor recommends a specific DoD PKI certificate profile.

Click on the appropriate profile and navigate to the next page.

1.3.4 Uploading the PKCS#10 Certificate Signing Request

After you have selected the certificate profile, you will see a page that allows you to upload the PKCS#10 message (Certificate Signing Request) in Section 1.2.2. When prompted, copy and paste the contents of the PKCS#10 message and make sure that "PKCS#10" is selected as the Certificate Request Type. Also, be sure to include the "-----BEGIN CERTIFICATE REQUEST-----" and "------END CERTIFICATE REQUEST-----" lines when pasting the PKCS#10 message.



Certificate Profile - New SSL Enrollment form

New SSL server enrollment form to include Multi-SAN with Extended Key Usage

Inputs

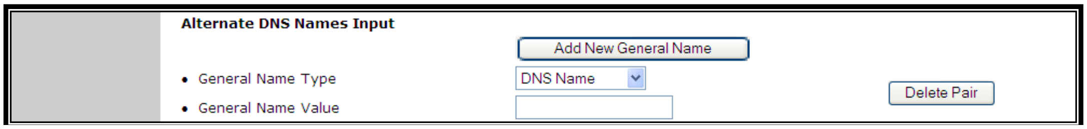
Certificate Request Input

- =Certificate Request Type: PKCS#10
- Certificate Request:

```
BiMlv
tb7K3CHfgw5WagWnLl8Lb+ccvKZZl+8CAwEAAaAAMA0GCSqGSIb3DQEBBAU
AA4GB
AHpoRp5YS55CZpy+wdigQEwjL/wSluvo+WjtpvP0YoBMJu4VMKeZi405R7o
8oEwi
PdlrrliKNknFmHKIaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrSRo3NKfg1bd
09D1K
9rsQkRc9Urv9mRBIsredGnYECNeRaK5R1yzpOowninXC
-----END CERTIFICATE REQUEST-----
```

1.3.5 Adding Additional Identities to the Certificate

If you have selected the New SSL Enrollment profile or the Multi-SAN profile (including the 2048 bit versions of these profiles), you will see a section called “Alternate DNS Names Input” below the Certificate Request Input section.



Alternate DNS Names Input

- General Name Type: DNS Name
- General Name Value:

If the UC equipment needs to be identified by more than one name (for example multiple IP addresses or DNS names), you can add additional names using the “Alternate DNS Names Input” section. The added names impact a field known as the “Subject Alternative Name” (SAN) field in the certificate. The Subject Alternative Name field in an X.509 certificate allows multiple identities, in addition to the X.509 “Subject” field (which only supports one identity via its “Common Name” field), to be used to identify a subject. Put another way, it is an “alternative” means to identify the “subject” of a DoD PKI certificate.

In general, use caution before adding additional identities to a certificate’s Subject Alternative Name field because some equipment may not support use of this feature or correctly process the additional identities. For instance, some equipment may only examine the Subject field and ignore any additional identities in the Subject Alternative Name field. Confirm the correct way to populate the Subject Alternative Name field with your vendor, assuming that use of this field is even required by the equipment. UC Equipment may use certificates for web servers, protecting call signaling, or IPSec tunnels, and each application has its own way of handling certificates to include the Subject Alternative Names field.

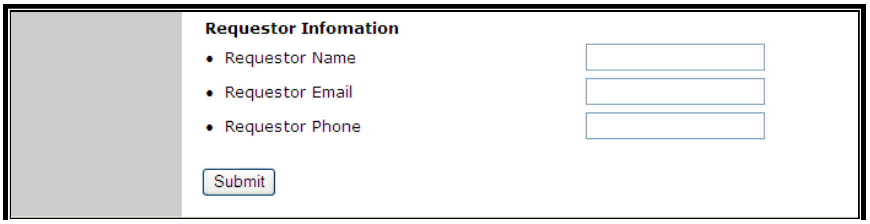
Presently the DoD PKI allows DNS names, IP addresses, URI Names, or Directory Names to be used for additional identities. For UC equipment, use of the IP address (IPv4 or IPv6 address) and DNS name (for example, ebc1.lackland.af.mil) types will be the most common, with DNS name (Fully Qualified Domain

Name) being preferred. You can submit up to 50 additional identities to include in a certificate, but note that not all equipment can support large numbers of Subject Alternative Names.

When the Subject Alternative Name field is present in the certificate, the DoD PKI will automatically make the first Subject Alternative Name value in a certificate equal to the value of the "Common Name" in the Subject field. For example, if the Common Name value of the Subject field contains "192.168.4.245", the identity "192.168.4.245" would be the first entry in the Subject Alternative Name field and would precede any other identities present.

1.3.6 Inputting the Requester's Contact Information

Finally, input the name, e-mail address, and phone number to associate with this certificate request and hit "Submit".



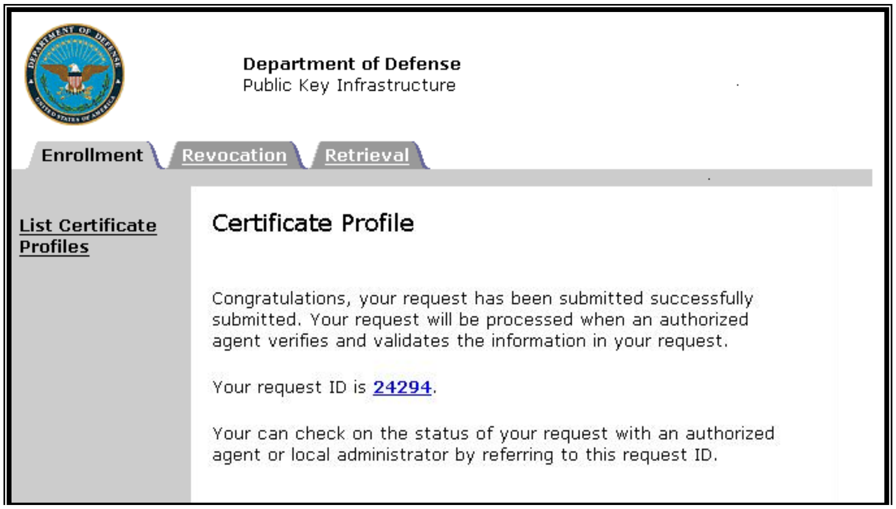
Requestor Infomation

- Requestor Name
- Requestor Email
- Requestor Phone

The "Requestor Information" must be the actual system administrator posting this request. Also note that the "Requestor" must be the same person identified as the System Administrator on the DoD PKI certificate requirement forms sent to the Local Registration Authority (LRA). See section 1.4 for additional information on contacting your LRA and submitting your request.

1.3.7 Confirmation of Your Submitted Request

Once you have successfully submitted the certificate request, you should see a screen similar to the following. Take note of the Request Identifier ("request ID") just in case there is an issue delivering the request confirmation to your e-mail account. You will need this Request Identifier later when submitting the request to your Local Registration Authority (LRA):



Department of Defense
Public Key Infrastructure

Certificate Profile

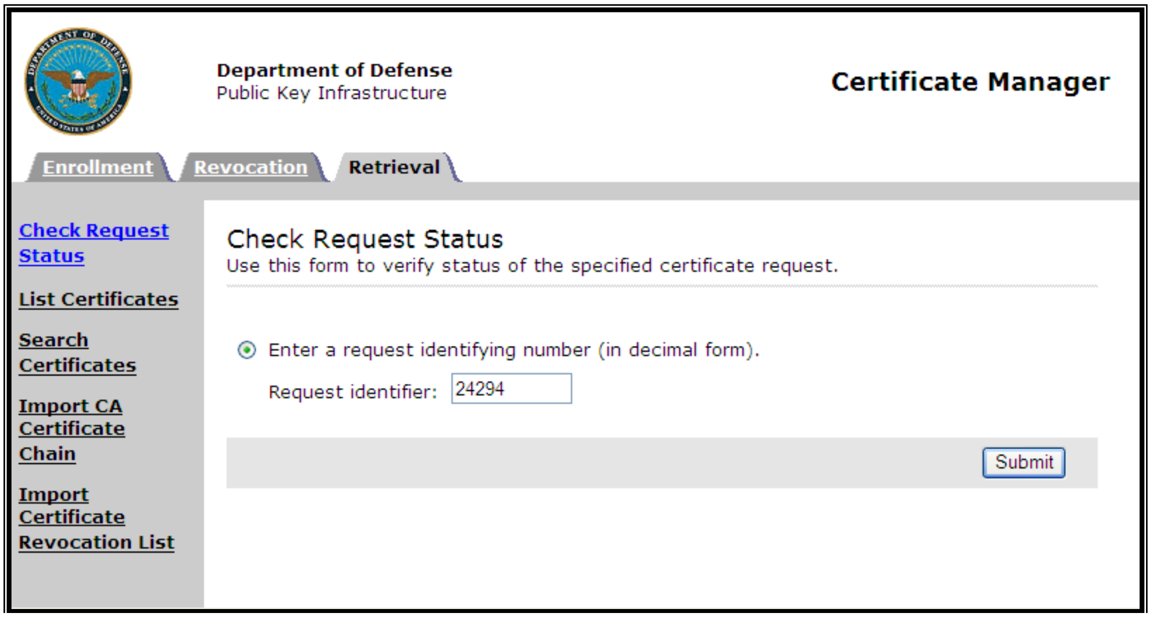
Congratulations, your request has been submitted successfully submitted. Your request will be processed when an authorized agent verifies and validates the information in your request.

Your request ID is 24294.

Your can check on the status of your request with an authorized agent or local administrator by referring to this request ID.

1.3.8 Checking the Status of a Submitted Certificate Request

If you need to go back and check on the status of an existing request, go back to the website for the CA that you used and navigate to the "Retrieval" tab. Click "Check Request Status" and input the Request Identifier as shown in the following figure and hit "Submit". You can also check with your Local Registration Authority to find out the status of your certificate request as well.



Check Request Status

Use this form to verify status of the specified certificate request.

● Enter a request identifying number (in decimal form).

Request identifier: 24294

1.4 Submitting the Certificate Request to a Local Registration Authority

Even though you have submitted the Certificate Signing Request to the DoD PKI Certificate Authority, the certificate will NOT be issued by the DoD PKI CA until you have submitted the certificate request to your Local Registration Authority (LRA). This allows the LRA to verify your request and this is typically the only way that the LRA knows that you have a certificate request pending. Unfortunately, each LRA may have different steps for submitting your certificate request depending on the organization to which you belong. The complete steps for submission of the request to each LRA have not been provided here, however the following sections note reference documents and contacts that can assist with this step of the process.

1.4.1 Tips for Expediting Your Certificate Request

After the certificates have been uploaded to the DoD PKI CA website, call your LRA for a second time to let them know that one or more certificate requests are pending. Also, provide the LRA with the Request Number(s) observed during the confirmation of your uploaded request (See Section 1.3.7). This will assist your LRA with identifying the specific request(s) requiring expedited service.

1.4.2 Submitting the Certificate Request to the Air Force LRA

To call the Air Force CAC/PKI Help Desk use the following number:

Air Force PKI Help Desk: 1-210-925-2521 (Commercial)

You can find a list of Local Registration Authorities (LRA) at the following website:

https://afpki.lackland.af.mil/html/lracontacts.asp (this site is accessible from .mil domains only)

You can also send e-mail to following address to find your nearest LRA and obtain instructions for downloading the "DoD PKI Server Certificate Requirement" document, which must be completed and submitted to the LRA before the certificates are issued:

afpki.ra@lackland.af.mil

Additional Air Force PKI support is available from the Air Force PKI help desk:

https://afpki.lackland.af.mil/html/help_desk.asp (this site is accessible from .mil domains only)

1.4.3 Submitting the Certificate Request to the Army LRA

For the Army, you will need to either become approved as the Trust Agent (TA) for your installation/activity in order to request certificates, or you will need to contact your Trust Agent to submit the request on your behalf. Alternatively, the Trust Agent may have appointed a Delegated Agent to perform PKI registration authorizations, so the Delegated Agent can be used as well. For more information, you can contact:

Army PKI-E Registration Authority
Hours of Operation:
M-F 0630-1600 MST / 1330-2300 Zulu
Email: ctnosc.pki@us.army.mil

24/7 CONUS TNOSC Service Desk
Toll Free 1-800-305-3036
DSN 312-538-6798
CML: 520-538-6798

Army CAC/PKI Helpdesk
NETCOM OM-IA CAC/PKI
Email: iacacpki.helpdesk@us.army.mil
Phone: 703-602-7514
Phone: 866-738-3222
DSN 332-7514

1.4.4 Submitting the Certificate Request to the Navy LRA

The phone numbers for Navy PKI helpdesk support are as follows:

SPAWAR Integrated Support Center Helpdesk
https://infosec.navy.mil/PKI/
Email: itac@infosec.navy.mil
Phone: 800-304-4636
DSN 588-4286

For the Navy, you can also find a list of LRAs at the following website (CAC authorization required): **https://infosec.navy.mil**. Navigate to the PKI tab (Top Left), LRA Link (on left side), then LRA Locator (updated annually). LRA Locator list will provide a comprehensive list of LRAs by command; additional information includes a POC, email and phone number. NAVY-wide technical support can be contacted at itac@infosec.navy.mil.

Once the CSR has been generated and submitted to the DoD PKI CA Website you will receive a request ID Number. The request ID number, CA number, and the FQDN of the server will need to be submitted to the LRA for verification and approval.

1.4.5 Submitting the Certificate Request to the US Marine Corp LRA

The US Marine Corp Operations Helpdesk can be reached at the following e-mail and phone number:

USMC RA Operations Helpdesk
Email: raoperations@mcnosc.usmc.mil
Phone: 703-432-0394

1.4.6 Submitting the Certificate Request to the DISA Registration Authority

The DISA registration authority can be reached at the following e-mail address:

E-mail: disaraoperations@disa.mil

1.4.7 Submitting the Certificate Request for All Other Organizations

Navigate to the following website to find additional contacts for your organization as well as addition DoD PKI support links:

http://iase.disa.mil/pki-pke/contact.html

You can also use the contacts listed in Section 2.1 to determine your assigned Local Registration Authority and then contact them to find out the procedures for submitting your DoD PKI certificate request.

1.5 Loading the Trust Chains and CRL/OCSP Pointers into Equipment

1.5.1 Loading DoD PKI Trust Chains

Prior to loading any requested certificates issued by the DoD PKI CA, it is recommended that administrators load certificates into UC equipment in the following order to achieve the best results:

Suggested Order for Loading DoD PKI Certificates into UC Equipment	
Order	**Certificate Type**
First	DoD PKI Root Certificate (DoD PKI Root 2)
Second	DoD PKI Intermediate CA Certificates (CA-21 and/or CA-22)
Third	Configure OCSP responder URL; verify OCSP responder connectivity at this point - or - If CRLs are used instead of OCSP, configure CRL distribution points and verify that CRLs can be retrieved at this point
Fourth	Any other required certificates issued by the DoD PKI CA to the device

This loading order gives equipment the opportunity to verify certificates as they are loaded instead of at later time. If the equipment determines that a problem exists as the credentials are loaded, detection at this stage will provide an administrator the ability to more efficiently troubleshoot issues. For example, equipment may be able to detect signature or corruption issues on a loaded certificate by using the pre-loaded root or intermediate CA certificate to verify signatures. Also see Appendix A for information on issues that could arise as certificates are transferred between different machines and media.

1.5.2 Configuration of CRLs and OCSP Responders

Configuration of CRLs and OCSP Responders will vary depending on the UC equipment type. The "deployment guide" specific to the UC product should be consulted for the exact configuration details. Also, please see Sections 2.2 and 2.3 for more detailed information on the operation of the DoD PKI CRLs and OCSP Responders. In short, UC equipment will be expected use to the following locations to retrieve DoD PKI OCSP Responses and DoD PKI CRLs. Note that as of November 1, 2010, the DoD PKI OCSP Responders only utilize the Delegated Trust Model (DTM). For a more detailed explanation of DTM, see Section 2.3.3.

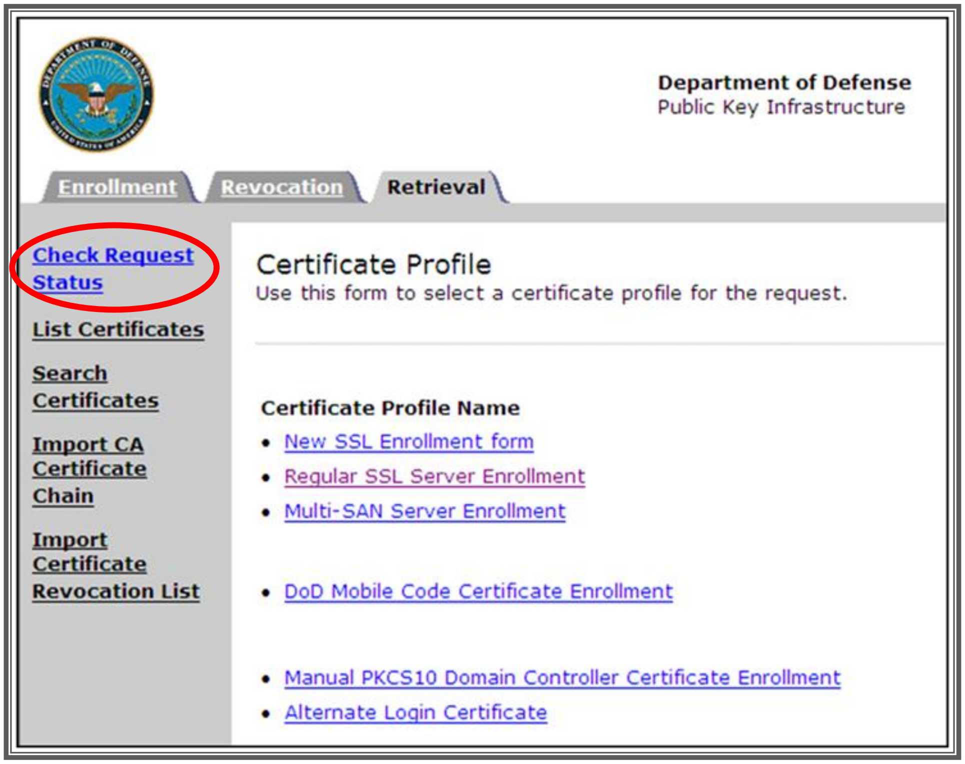
Locations for DoD PKI OCSP Responder and CRL Distribution Point for UC Devices		**Purpose**
DoD PKI OCSP Responder	http://ocsp.disa.mil (To see the IP addresses that correspond to this URL, see Section 2.3.5) (**Note:** The above URL corresponds to 4 CONUS OCSP responder sites. Additional OCSP URLs for OCONUS OCSP responders exist, however if these are configured, the DoD PKI PMO recommends still configuring ocsp.disa.mil as backup. See Section 2.3.5 for more information: http://oconusocsp.disa.mil [EUR] http://oconusocsp2.disa.mil [PAC] OCONUS locations can still use the CONUS OCSP URL without issue.) (**Note:** As of November 1, 2010, the DoD PKI has deactivated the http://ocsp-legacy.disa.mil URL intended to support older OCSP clients that did not yet support DTM)	Used to check the status of a certificate and obtain a real-time response. The response is signed using a certificate issued to the OCSP responder by a DoD PKI CA. When OCSP responses are signed in this manner, this is known as the delegated trust model or DTM. (See Section 2.3.3 for more information on DTM)
DoD PKI CRL Distribution Point for DoD PKI Root CA-2	http://crl.disa.mil/getcrl?DoD%20Root%20CA%202	Used to determine the intermediate CAs whose certificates have been revoked
DoD PKI CRL Distribution Point for Intermediate CA-21	http://crl.disa.mil/crl/DODCA_21.crl (preferred because this is a static URL) or http://crl.disa.mil/getcrl?DoD%20CA-21 (usable but not preferred because it is dynamic and will be deprecated in the future – date is TBD)	Used to determine the list of certificates issued to devices by CA-21 that have been revoked
DoD PKI CRL Distribution Point for Intermediate CA-22	http://crl.disa.mil/crl/DODCA_22.crl (preferred because this is a static URL) or http://crl.disa.mil/getcrl?DoD%20CA-22 (usable but not preferred because it is dynamic and will be deprecated in the future – date is TBD)	Used to determine the list of certificates issued to devices by CA-22 that have been revoked
DoD PKI CRL Distribution Point for Intermediate CA-27	http://crl.disa.mil/crl/DODCA_27.crl (active starting Dec 2011)	Used to determine the list of certificates issued to devices by CA-27 that have been revoked
DoD PKI CRL Distribution Point for Intermediate CA-28	http://crl.disa.mil/crl/DODCA_28.crl (active starting Dec 2011)	Used to determine the list of certificates issued to devices by CA-28 that have been revoked

Also note that CRLs for all of the CAs can be manually retrieved via the following URL:

https://crl.gds.disa.mil/

1.6 Retrieving and Loading Your DoD PKI CA Issued Certificate

Once you receive e-mail confirmation that your certificate is waiting, you can log back into the appropriate Certificate Authority website and retrieve your certificate. Open your web browser and navigate to the appropriate CA site. Select the "Retrieval" tab and then select "Check Request Status."



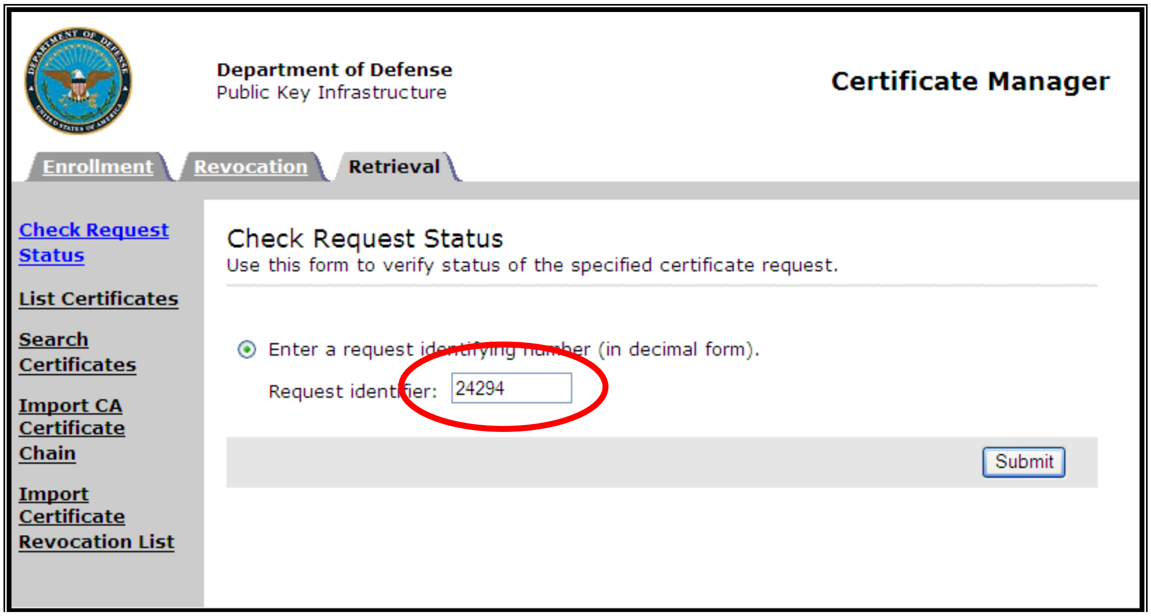
Certificate Profile

Use this form to select a certificate profile for the request.

Certificate Profile Name

- New SSL Enrollment form
- Regular SSL Server Enrollment
- Multi-SAN Server Enrollment
- DoD Mobile Code Certificate Enrollment
- Manual PKCS10 Domain Controller Certificate Enrollment
- Alternate Login Certificate

Next, input the Request ID number (for example "24294") recorded from the previous step in Section 1.3.7. Click "Submit" and continue to the next page.



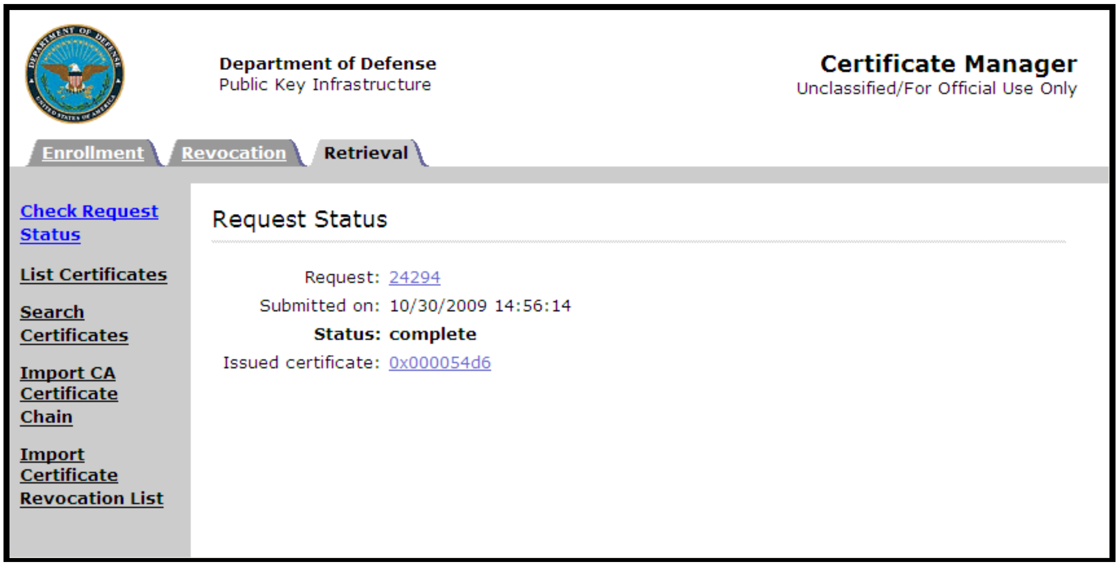
Check Request Status

Use this form to verify status of the specified certificate request.

● Enter a request identifying number (in decimal form).

Request identifier: 24294

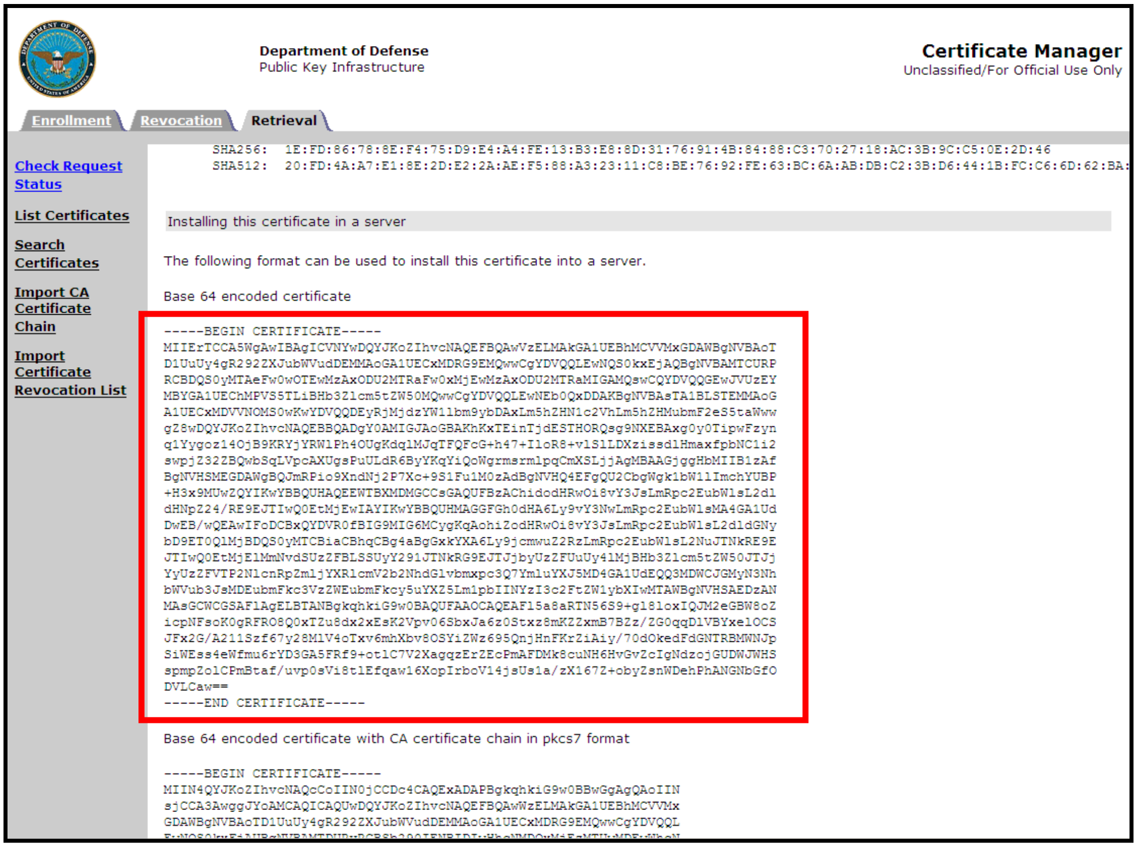
If successful, you should a screen showing the "Request Status." This screen should show a status of "complete" at this point, and you can then click on the serial number next to the "Issued Certificate" to see the generated certificate.



Request Status

Request: 24294
Submitted on: 10/30/2009 14:56:14
Status: complete
Issued certificate: 0x000054d6

A page displaying the certificate contents will appear. Scroll down to the "Installing this certificate in a server" section to view the certificate in a format acceptable for installation into an UC component.



```
SHA256:  1E:FD:86:78:8E:F4:75:D9:E4:A4:FE:13:B3:E8:8D:31:76:91:4B:84:88:C3:70:27:18:AC:3B:9C:C5:0E:2D:46
SHA512:  20:FD:4A:A7:E1:8E:2D:E2:2A:AE:F5:88:A3:23:11:C8:BE:76:92:FE:63:BC:6A:AB:DB:C2:3B:D6:44:1B:FC:C6:6D:62:BA:
```

Installing this certificate in a server

The following format can be used to install this certificate into a server.

Base 64 encoded certificate

```
-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgICVNYwDQYJKoZIhvcNAQEFBQAwVzELMAkGA1UEBhMCVVMxGDAWBgNVBAoT
D1UuUy4gR292ZXJubWVudDEMMAoGA1UECxMDRG9EMQwwCgYDVQQLEwNQS0kxEjAQBgNVBAMTCURP
RCBDQS0yMTAeFw0wOTEwMzAxODU2MTRaFw0xMjEwMzAxODU2MTRaMIGAMQswCQYDVQQGEwJVUzEY
MBYGA1UEChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNEb0QxDDAKBgNVBAsTA1BLSTEMMAoG
A1UECxMDVVNOMS0wKwYDVQQDEyRjMjdzYW1lbm9ybDAxLm5hZHN1c2VhLm5hZHMubmF2eS5taWww
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKhKxTEinTjdESTHORQsg9NXEBAxg0y0TipwFzyn
q1Yygoz14OjB9KRYjYRWlPh4OUgKdqlMJqTFQFcG+h47+IloR8+vlSlLDXzissdlHmaxfpbNC1i2
swpjZ32ZBQwbSqLVpcAXUgsPuULdR6ByYKqYiQoWgrmsrmlpqCmXSLjjAgMBAAGjggHbMIIB1zAf
BgNVHSMEGDAWgBQJmRPio9XndNj2P7Xc+9S1Fu1M0zAdBgNVHQ4EFgQU2CbgWgk1bW1lImchYUBP
+H3x9MUwZQYIKwYBBQUHAQEEWTBXMDMGCCsGAQUFBzAChidodHRwOi8vY3JsLmRpc2EubWlsL2dl
dHNpZ24/RE9EJTIwQ0EtMjEwIAYIKwYBBQUHMAGGFGh0dHA6Ly9vY3NwLmRpc2EubWlsMA4GA1Ud
DwEB/wQEAwIFoDCBxQYDVR0fBIG9MIG6MCygKqAohiZodHRwOi8vY3JsLmRpc2EubWlsL2dldGNy
bD9ET0QlMjBDQS0yMTCBiaCBhqCBg4aBgGxkYXA6Ly9jcmwuZ2RzLmRpc2EubWlsL2NuJTNkRE9E
JTIwQ0EtMjElMmNvdSUzZFBLSSUyY291JTNkRG9EJTJjbyUzZFUuUy4lMjBHb3Zlcm5tZW50JTJj
YyUzZFVTP2NlcnRpZmljYXRlcmV2b2NhdGlvbmxpc3Q7YmluYXJ5MD4GA1UdEQQ3MDWCJGMyN3Nh
bWVub3JsMDEubmFkc3VzZWEubmFkcy5uYXZ5Lm1pbIINYzI3c2FtZW1ybXIwMTAWBgNVHSAEDzAN
MAsGCWCGSAFlAgELBTANBgkqhkiG9w0BAQUFAAOCAQEAFl5a8aRTN56S9+gl8loxIQJM2eGBW8oZ
icpNFsoK0gRFRO8Q0xTZu8dx2xEsK2Vpv06SbxJa6z0Stxz8mKZZxmB7BZz/ZG0qqDlVBYxelOCS
JFx2G/A211Szf67y28MlV4oTxv6mhXbv8OSYiZWz695QnjHnFKrZiAiy/70dOkedFdGNTRBMWNJp
SiWEss4eWfmu6rYD3GA5FRf9+otlC7V2XagqzErZEcPmAFDMk8cuNH6HvGvZcIgNdzojGUDWJWHS
spmpZolCPmBtaf/uvp0sVi8tlEfqaw16XopIrboV14jsUs1a/zX167Z+obyZsnWDehPhANGNbGfO
DVLCaw==
-----END CERTIFICATE-----
```

Base 64 encoded certificate with CA certificate chain in pkcs7 format

```
-----BEGIN CERTIFICATE-----
MIIN4QYJKoZIhvcNAQcCoIIN0jCCDc4CAQExADAPBgkqhkiG9w0BBwGgAgQAoIIN
sjCCA3AwggJYoAMCAQICAQUwDQYJKoZIhvcNAQEFBQAwWzELMAkGA1UEBhMCVVMx
GDAWBgNVBAoTD1UuUy4gR292ZXJubWVudDEMMAoGA1UECxMDRG9EMQwwCgYDVQQL
```

The certificate shown in this section can then be loaded into the UC component via its user configuration interface. The process for loading the certificate into equipment will vary depending on how the equipment accepts certificates. Some equipment may allow loading of the certificate by copying and pasting the certificate into a configuration page. If this is the case, be sure to include the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines if the UC component requires it since this is considered to be part of the certificate's format (known as PEM or PKCS#7). For equipment that requires the certificate to be loaded from a file, copy the certificate into a file on the file system and hit "Save". Next, navigate to that file and select it using the equipment's configuration interface.

You may need to use the "Base 64 encoded certificate" format (just the certificate itself) or the "Base 64 encoded certificate with CA certificate chain in pkcs7 format" (certificate plus full certificate chain to the root certificate authority). The format used will depend on the requirements of your particular system. Consult the vendor's documentation for more information on the correct format to use.

Always process the base 64 representation of the certificate using plaintext editors and formats. Avoid rich text editors (e.g. MS Word) that might insert extraneous spaces, metadata, or characters that might corrupt the certificate representation.

2 Other Frequently Asked Questions

This section contains answers to frequently asked questions related to the use of the DoD PKI with the equipment comprising the DoD Unified Capabilities architecture.

2.1 How can I contact the DoD PKI PMO to obtain assistance?

You can send requests for assistance to DoD PKE Engineering Support at the following e-mail address: **<pke_support@disa.mil>**.

You can also obtain support by calling the DoD PKI help desk in Oklahoma. This Help Desk operates around-the-clock (24x7) services for PKI users at all levels and will take calls or e-mails from an DoD PKI user experiencing a problem with PKI. This help desk can be reached as follows:

PKI Help Desk Oklahoma City, OK Support:
E-Mail: Okc-dodost@csd.disa.mil
Phone (Commercial): 1-800-490-1643
Phone (DSN): 339-5600

Finally, you can obtain additional information on the DoD PKI and Public Key Enablement (PKE) at the following website:

http://iase.disa.mil/pki/index.html

2.2 Certificate Revocation Lists (CRLs)

2.2.1 What is a Certificate Revocation List?

The DoD PKI also provides the capability to invalidate previously issued certificates via the use of certificate revocation lists (CRLs). A CRL is a list of certificate identification numbers that has been formatted in a standard manner and signed by a certificate authority (CA). Each number on the list corresponds to the certificate serial number for the certificate that has been revoked.

2.2.2 How can I obtain a Certificate Revocation List from the DoD PKI?

Devices and administrators can obtain CRLs from CRL Distribution Points. A CRL Distribution Point (CDP) is a server that accepts requests for CRLs using a designated communication protocol (like HTTP) and responds by providing the latest CRL for the associated certificate authority. For the DoD PKI, CRL Distribution Points will support retrieval of CRLs using either the Hypertext Transfer Protocol (HTTP) or the Lightweight Directory Access Protocol (LDAP). As discussed in Section 2.2.4, HTTP is the preferred approach.

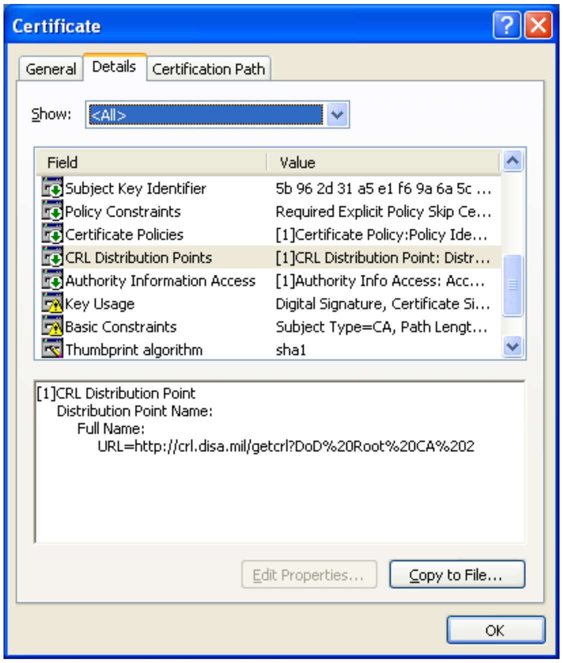
The CRL Distribution points applicable to your installation will vary depending on the certificate authorities that issued certificates to the communicating devices in your system. Most UC devices using the DoD PKI will only need to retrieve DoD PKI CRLs corresponding to DoD PKI Root Certificate Authority 2 and Intermediate Certificate Authorities 21 and 22 in the near term. However, the DoD PKI PMO is continually enhancing the DoD PKI's capabilities as new Certificate Authorities become operational.

To view the CRL yourself, any web browser can be used to download a CRL from a CRL distribution point. As an example, the URL to retrieve the CRL for DoD PKI CA-2 via HTTP (Port 80) is as follows (see Section 1.5.2 for other URLs relevant to UC devices):

http://crl.disa.mil/getcrl?DoD%20Root%20CA%202

(If you put this link into your web browser, you will be able to download the CRL to a file.)

For intermediate CA certificates, you can also determine the URL of the CRL Distribution Point for your specific CA by opening the CA’s certificate in Microsoft Windows’ certificate viewer. Click on the “Details” tab and you should see a screen that resembles the following:



Show: <All>

Field	Value
Subject Key Identifier	5b 96 2d 31 a5 e1 f6 9a 6a 5c ...
Policy Constraints	Required Explicit Policy Skip Ce...
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Certificate Si...
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint algorithm	sha1

```
[1]CRL Distribution Point
    Distribution Point Name:
        Full Name:
            URL=http://crl.disa.mil/getcrl?DoD%20Root%20CA%202
```

Click on the “CRL Distribution Points” fields to examine the details of this field. The URLs contained in this field will indicate the Fully Qualified Domain Name (FQDN) for the CRL distribution point and the scheme (HTTP, LDAP, or either if multiple options are present) used to retrieve CRLs from the CRL Distribution Point.

For end device certificates, the steps for viewing the CRL distribution point in Microsoft Windows are exactly the same as those shown in the preceding paragraphs. Note that for end device DoD PKI certificates, an intermediate CA (21 or 22 for instance) publishes the CRL, not DoD PKI Root-CA 2.

2.2.3 What If I Need an IP Address for the CRL Distribution Point?

At present, the FQDN “crl.disa.mil” maps to the following IP addresses:

IP Addresses Corresponding to crl.disa.mil	
DECC Mechanicsburg	156.112.102.122 [Old IP address: 214.21.15.23 – not valid after Sep 2011]
DECC Oklahoma City	156.112.110.122 [Old IP address: 152.229.242.172 – not valid after Sep 2011]

It is recommended that the FQDN “crl.disa.mil” be configured for use in UC equipment instead of a single IP address in case these IP addresses are changed in the future or a site is taken offline for maintenance.

2.2.4 Should I Use HTTP or LDAP to Retrieve CRLs?

If you have the choice, use HTTP when possible to receive CRLs due to the bandwidth intense nature of LDAP. LDAP is an older way to retrieve CRLs from the DoD PKI whereas HTTP is the approach recommended by most organizations including the DoD PKI PMO.

2.2.5 How Often Should CRLs Be Retrieved?

The DoD PKI CRLs are published twice per day. However, to avoid congestion, the DoD PKI PMO generally recommends that organizations retrieve CRLs no more than once every 24 hours. This recommendation is based on the information at the following link (right hand side of page 2):

http://iase.disa.mil/pki/pke/documents/slick_sheet3-certificate_validation_final.doc

In some cases, the DoD PKE office may still recommend that CRLs be retrieved twice per day if your mission or program necessitates more timely DoD PKI updates. The DoD PKI PMO also recommends that, where possible, enclaves cache CRLs so that only a single retrieval per site is necessary. To assist with CRL caching, the DoD PKE Engineering Support team has developed a tool called “CRLAutoCache” that can retrieve a CRL and then publish it to local servers in a variety of formats. Visit http://iase.disa.mil/pki/pke for more information.

2.3 Online Certificate Status Protocol (OCSP)

2.3.1 What is OCSP?

OCSP stands for “Online Certificate Status Protocol.” This protocol allows a device to obtain real-time information on the status (e.g. whether or not the certificate has been revoked) of a given certificate. The DoD PKI supports the use of both OCSP and Certificate Revocation Lists (CRLs).

2.3.2 What is an OCSP Responder?

An "OCSP Responder" is a server that accepts OCSP queries and provides OCSP formatted responses indicating the validity status of queried certificate. OCSP is transmitted and received as a payload of HTTP, so OCSP traffic should be considered equivalent to web traffic from a protocol treatment/firewall rule standpoint. The DoD PKI PMO has deployed a set of OCSP responders to provide responses for DoD PKI certificates. To configure your equipment so that it can reach the DoD PKI OCSP Responder, you will need the URL or IP address for the OCSP responder.

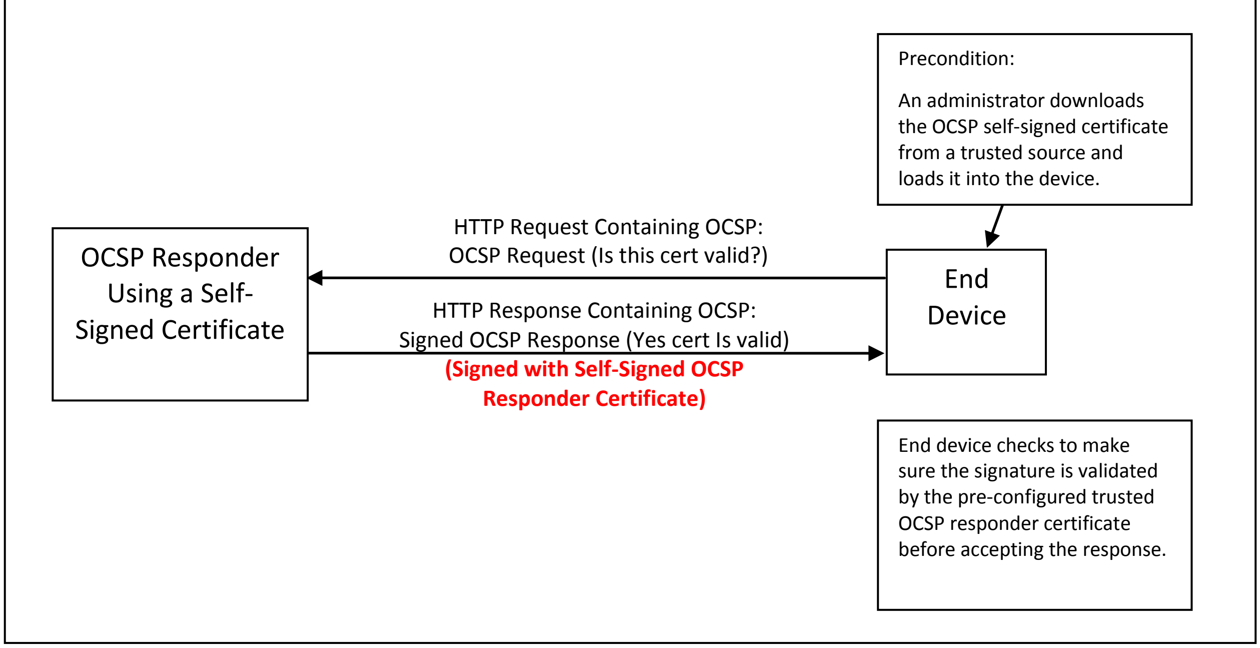
The DoD PKI OCSP responders retrieve revocation information from the DoD PKI CRLs published by the DoD PKI certificate authorities. The DoD PKI OCSP responders pull the latest CRLs every several times per day in order to keep the OCSP responses up-to-date, but there is a small lag between the time that a certificate is revoked and the time that an OCSP responder updates it revocation information.

2.3.3 What is the OCSP Delegated Trust Model (DTM)?

Until the middle of 2010, DoD PKI CAs did not issue a certificate to OCSP responders. Instead, a "self-signed" certificate was generated and provided for the OCSP responders, which had to be manually retrieved and configured. A "self-signed" certificate cannot be delivered "over the wire" via an untrusted channel (like plain HTTP), because there is no way to validate that the "self-signed" certificate has not been modified in transit.

The Delegated Trust Model (also known as the IETF RFC 2560 "Authorized Responder") or DTM resolves this issue. With DTM, a DoD PKI certificate authority issues a certificate to the OCSP responder. Because the OCSP responder's certificate is signed by a trusted authority, it can be delivered via an untrusted channel (such as HTTP). If the certificate contained in the response is modified while in transit, a device can still detect any modifications because the signature on the response and/or certificate will no longer calculate correctly. As a result of DTM, the OCSP responder certificate no longer has to be separately downloaded and can be delivered "over the wire" to the device during the typical OCSP request/response protocol. (Note that OCSP relies on HTTP to transmit OCSP requests and responses as HTTP payloads).

The difference between the DTM and self-signed OCSP responder approaches is illustrated by the following diagrams:



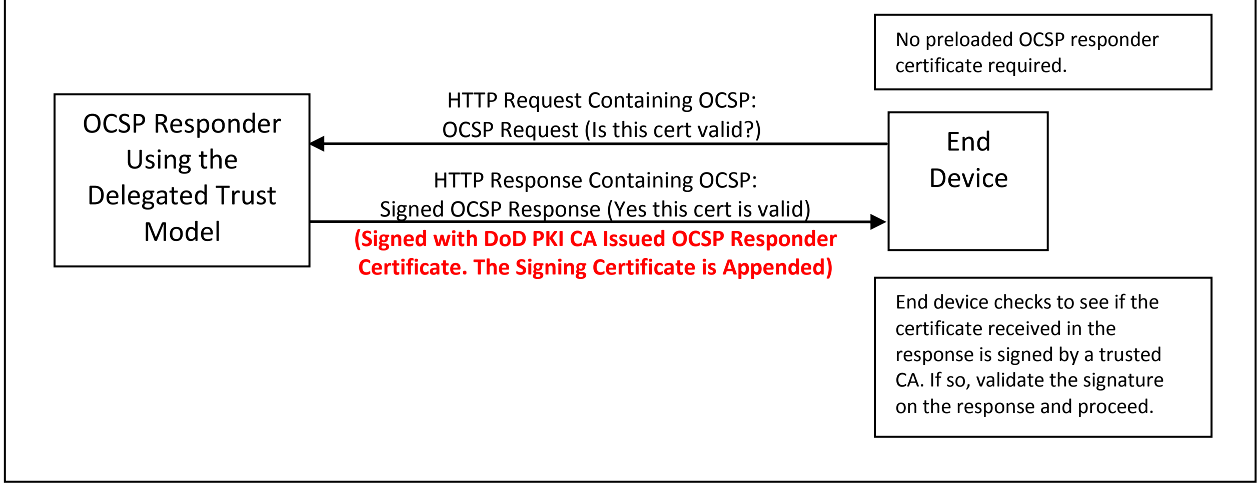
OCSP Responder Using a Self-Signed Certificate

OCSP Responder Using a Self-Signed Certificate
End Device
HTTP Request Containing OCSP: OCSP Request (Is this cert valid?)
HTTP Response Containing OCSP: Signed OCSP Response (Yes cert Is valid)
(Signed with Self-Signed OCSP Responder Certificate)

Precondition:

An administrator downloads the OCSP self-signed certificate from a trusted source and loads it into the device.

End device checks to make sure the signature is validated by the pre-configured trusted OCSP responder certificate before accepting the response.



OCSP Responder Using the Delegated Trust Model (DTM)

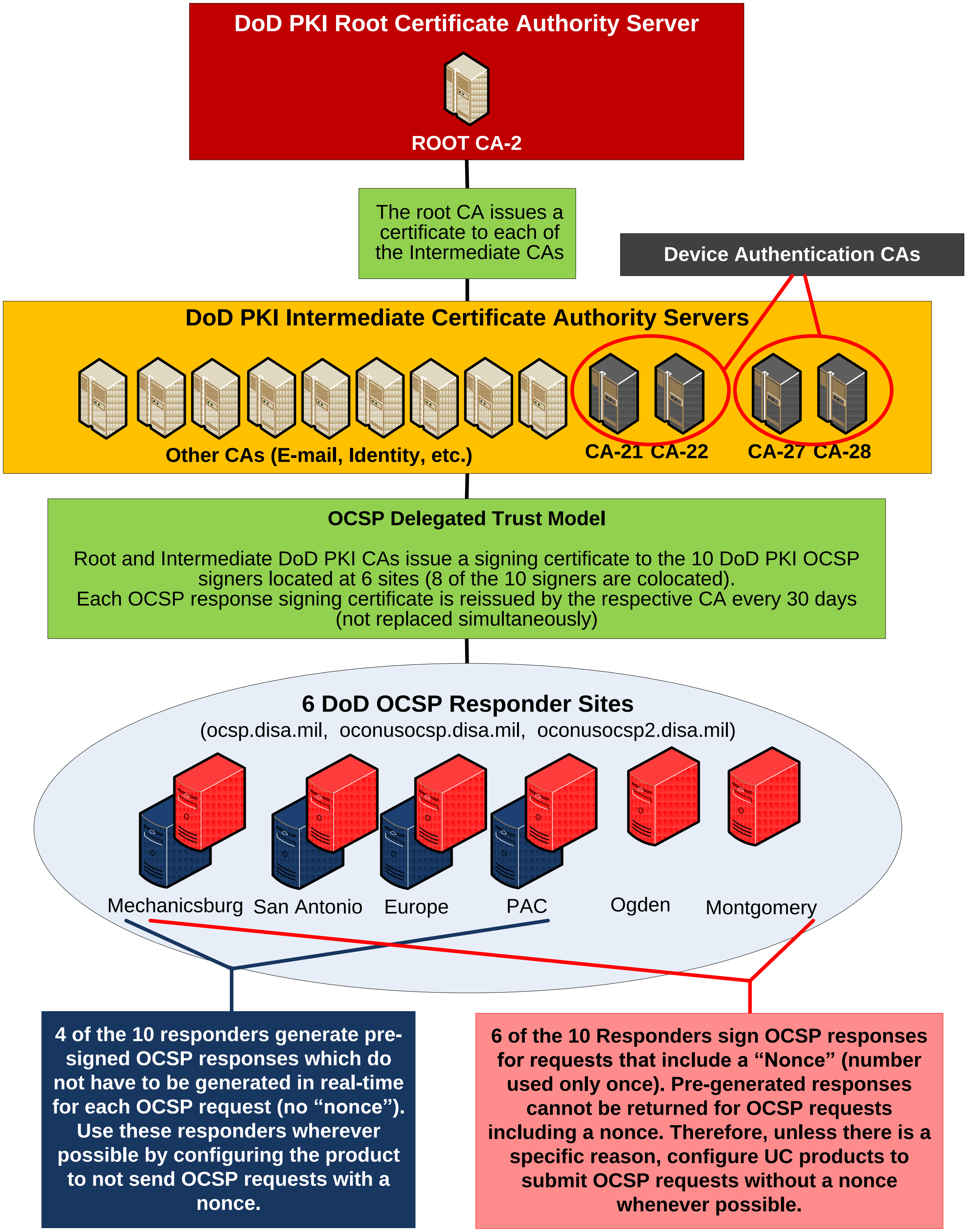
OCSP Responder Using the Delegated Trust Model
End Device
HTTP Request Containing OCSP: OCSP Request (Is this cert valid?)
HTTP Response Containing OCSP: Signed OCSP Response (Yes this cert is valid)
(Signed with DoD PKI CA Issued OCSP Responder Certificate. The Signing Certificate is Appended)

No preloaded OCSP responder certificate required.

End device checks to see if the certificate received in the response is signed by a trusted CA. If so, validate the signature on the response and proceed.

Products utilizing DoD PKI provided OCSP services are now required to support the DTM approach in addition to the tradition “self-signed” or “trusted responder” approach.

The following figure provides a more comprehensive illustration of how the DoD PKI implements the OCSP Delegated Trust Model.



DoD PKI Root Certificate Authority Server
ROOT CA-2
Device Authentication CAs
DoD PKI Intermediate Certificate Authority Servers
Other CAs (E-mail, Identity, etc.)
CA-21 CA-22
CA-27 CA-28
6 DoD OCSP Responder Sites
(ocsp.disa.mil, oconusocsp.disa.mil, oconusocsp2.disa.mil)
Mechanicsburg
San Antonio
Europe
PAC
Ogden
Montgomery

The root CA issues a certificate to each of the Intermediate CAs

OCSP Delegated Trust Model

Root and Intermediate DoD PKI CAs issue a signing certificate to the 10 DoD PKI OCSP signers located at 6 sites (8 of the 10 signers are colocated).
Each OCSP response signing certificate is reissued by the respective CA every 30 days (not replaced simultaneously)

4 of the 10 responders generate pre-signed OCSP responses which do not have to be generated in real-time for each OCSP request (no "nonce"). Use these responders wherever possible by configuring the product to not send OCSP requests with a nonce.

6 of the 10 Responders sign OCSP responses for requests that include a "Nonce" (number used only once). Pre-generated responses cannot be returned for OCSP requests including a nonce. Therefore, unless there is a specific reason, configure UC products to submit OCSP requests without a nonce whenever possible.

2.3.4 What are the URLs for the DoD PKI's OCSP Responders?

The URLs for the DoD PKI OCSP responders are listed in the table in Section 1.5.2. The TCP port associated with these URLs is HTTP port 80. Note that these are load-balanced URLs. In other words, each query transmitted to this URL is farmed out to any number of OCSP responders, not just a single responder. Since a high volume of OCSP requests are transmitted to this URL, load-balancing is used to improve responsiveness and availability.

2.3.5 What if I need an IP address for the OCSP Responder instead of a URL?

Some equipment may not yet support the use of Fully Qualified Domain Names (FQDNs) like "ocsp.disa.mil" when configuring the OCSP responder location and may only support configuration of the IP address. This scenario is NOT ideal because the DoD PKI PMO routinely takes down certain sites for maintenance. So use of the FQDN to locate OCSP resources is preferred. At the time of this document's writing, the "http://ocsp.disa.mil" URL resolves to one of four IP addresses depending on the geographic location from the DNS request originates. DNS queries to ocsp.disa.mil will only return one of the four IP addresses and not all four. For convenience, these addresses have been added to the table below:

IP Addresses Corresponding to http://ocsp.disa.mil	
OCSP Responder Location	**IP Address**
Mechanicsburg	164.235.152.142
Montgomery	164.235.104.142
Ogden	164.235.136.142
San Antonio	164.235.72.142

The previous four sites represent OCSP sites located in CONUS. There are also two OCSP responder sites located OCONUS as well. Because the OCONUS FQDNs map to only one site, if the OCONUS URLs are used, the DoD PKI PMO recommends additionally configuring the CONUS OCSP FQDN (ocsp.disa.mil), as a backup.

IP Address Corresponding to http://oconusocsp.disa.mil	
OCSP Responder Location	**IP Address**
Europe (EUR)	214.24.177.136

IP Address Corresponding to http://oconusocsp2.disa.mil	
OCSP Responder Location	**IP Address**
Pacific (PAC)	207.133.227.104

Again, it is recommended that the FQDN ocsp.disa.mil be used wherever possible, because these IP addresses may change in the future whereas the fully qualified domain name will remain the same even if IP address changes occur. Talk to your UC equipment vendor representative about adding support for configuring fully qualified domain names for the OCSP responder value if this is not already supported.

To manually view the IP address returned for the OCSP responders located at ocsp.disa.mil, use the following steps:
(The following instructions are for Windows XP, but these should be similar for other Windows variants)

1.) Go to the Windows "Start" Menu on the lower left-hand side of the screen
2.) Select "Run…"
3.) In the "Open" field type "cmd" and press "OK". A command prompt window should open.
4.) Type the command "nslookup ocsp.disa.mil" (or the appropriate FQDN) into the command prompt window
5.) The resulting address in the "Address:" field is the address to use for the OCSP responder

2.3.6 How can I obtain the self-signed certificate for the legacy OCSP responders?

As of November 1, 2010, the legacy DoD PKI OCSP Responders located at http://ocsp-legacy.disa.mil which utilized a "self-signed" certificate have now been deactivated. Products using DoD PKI provided OCSP services must now use the http://ocsp.disa.mil URL (which only supports the delegated trust model) or the appropriate OCONUS URLs. Therefore it is no longer necessary to obtain the legacy self-signed OCSP responder certificate.

2.3.7 Why do the OCSP Responders use HTTP instead of HTTPS?

DoD PKI OCSP Responders only use the hypertext transfer protocol (HTTP) instead of HTTP Secure (HTTPS) because OCSP responders delivered signed responses that can be authenticated using the certificate provided in the OCSP response. Therefore, it is not necessary to protect OCSP responses using the additional encryption or authentication features provided by HTTPS. For performance reasons, HTTP will likely continue to be used even as the DoD PKI evolves.

2.4 Which is better: OCSP or CRLs?

Even though both Certificate Revocation Lists distribution points and OCSP Responders provide the same information (the status of certificates), it is recommended to use OCSP whenever possible. A CRL can quickly become stale and CRLs can grow relatively large in size (several megabytes). OCSP allows for nearly real-time status information for a certificate and in general will not require nearly the same bandwidth needed to distribute CRLs.

2.5 Maintaining Valid DoD PKI Certificates in UC Equipment

2.5.1 How Often Do DoD PKI Certificates Need to Be Replaced?

All of the DoD PKI certificates utilized by the DoD PKI have expiration dates. It is important for administrators to take note of these expiration dates and ensure that new certificates are ordered and obtained prior to the expiration period. Note that beginning in 2011, the DoD PKI will begin to roll out new capabilities that allow for the ability to receive e-mail notifications when certificates are nearing expiration.

In general, administrators should plan to replace the certificates in UC components at the following intervals:

DoD PKI Certificate Type	Validity Period
DoD PKI Root Certificate Authority	Typically valid for around 25 years from the creation date. The current DoD PKI Root CA 2 will expire on Dec 5, 2029.
Intermediate Certificate Authority	Typically valid for between 6 - 10 years from the creation date (currently, DoD PKI CA-21 and CA-22 are valid from 2009 to 2015, however transition to DoD PKI CA-27 and CA-28 will occur will before the 2015 expiration)
OCSP Responder (DTM)	The DTM OCSP Responder certificate is changed every 30 days. However, no action is required by administrators because the latest OCSP responder certificate is included in every DTM OCSP response. DTM-enabled equipment will correctly use this certificate to validate responses without action from administrators.
End Entity (Users, Machines)	Typically valid for between 2 to 3 years from the date of issuance or less depending on mission requirements and the expiration date of the CA issuing the certificate (a CA cannot issue a certificate that has an expiration date beyond its own)

It is also important to ensure that any time sources (system clocks, Network Time Protocol (NTP) servers, etc.) are set to accurate values. Ensuring accurate time information ensures that equipment will not treat valid certificates as expired certificates and vice versa.

2.6 Should I Order 2048 Bit Certificates or 1024 Bit Certificates?

Due to the National Institute of Standards (NIST) mandates and concerns over the long term strength of 1024 bit certificates, the DoD PKI has transitioned from 1024 bit certificates to the stronger cryptographic strength 2048 bit certificates for the NIPRNET CAs. (The numbers 1024 and 2048 indicate the size of the RSA keys used in the certificates.) Only 2048 bit certificates can now be ordered from the NIRPRNET DoD PKI CAs. Note that this guidance applies to NIPRNET CAs, as SIPRNET CAs will issue 1024 bit certificates and CACs with 1024 bit certificates for an additional period of time.

Note that 1024 bit certificates can still be utilized beyond the 2010 date until they expire. Since certificates are typically issued with a maximum validity period of 3 years, administrators should expect to continue to see DoD PKI issued 1024 bit certificates in the field until the 2013 timeframe.

2.7 Where Can I Obtain All of the DoD PKI Certificate Authority Certificates?

Navigate to the following URL:

http://dodpki.c3pki.chamb.disa.mil/rootca.html

and then follow the instructions on the webpage to download the DoD PKI CA certificates.

There is also a graphical utility called InstallRoot which automatically installs all of the DoD PKI roots in Windows. It is available on the following websites:

http://iase.disa.mil/pki/pke
https://www.us.army.mil/suite/page/474113

2.8 What if I Only Need Test Certificates?

The Joint Interoperability Test Command (JITC) is most commonly used for testing DoD PKI certificates and DoD PKI services in a non-operational environment. The JITC operates a test root certificate authority, a test OCSP responder, and supports the capability to issue test certificates through its test certificate authority.

Note that any certificates issued by JITC must not be used for operational purposes.

2.8.1 Website for Submitting Certificate Requests to JITC

Currently JITC uses CA-21 to allow uploading of certificate signing requests. The website used to upload certificate requests is:

JITC CA-21: https://CA-21.c3pki.nit.disa.mil/ca/

Once on this website, the procedures for submitting the certificate signing request to the JITC CA are the same as those for requesting certificates via the operational certificate authority as specified in Sections 1.3.3 to 1.3.8. The procedures for retrieving the certificate through your Local Registration Authority will differ slightly however, as described in the next section.

2.8.2 Submitting the Test Certificate Request to Your LRA

After submitting your request to the JITC CA, the procedures for submitting your request to the Local Registration Authority to obtain the certificate will vary depending on your organization. In general, the requirements for obtaining JITC issued certificates should be less stringent than those for obtaining operational certificates.

For example, the Air Force only requires that requesters send an e-mail to *afpki.ra@lackland.af.mil* to identify who they are, the purpose for obtaining the test certificate, and the JITC CA # (for example 21) along with the request number the JITC CA provided during the confirmation step. Submission of a formal request form to the Air Force LRA is not required.

For all other organizations, please use the contacts provided in Section 1.4 to contact your Local Registration Authority, and then follow their instructions for obtaining test certificates from JITC.

2.8.3 Downloading Test Trust Chains

You can download the test trust chains and a CRL for the test JITC CA from the following websites:

https://crl.gds.nit.disa.mil/
https://ca-21.c3pki.nit.disa.mil/ca/rootCert.html

For additional information on JITC's test PKI services, you can go to the following website:

http://jitc.fhu.disa.mil/pki/

2.8.4 JITC OCSP Responder

JITC has established a test OCSP responder at the following link:

http://ocsp.nsn0.rcvs.nit.disa.mil

This responder uses the DTM approach and does not require the download of a self-signed certificate.

2.8.5 Points of Contact to Obtain Assistance with JITC Test Certificates

The contact information for the JITC GDS/JEDS Testing Lab, PKE Testing Lab, PKI Testing Lab can be found at the following link:

http://jitc.fhu.disa.mil/pki/point_of_contact.html

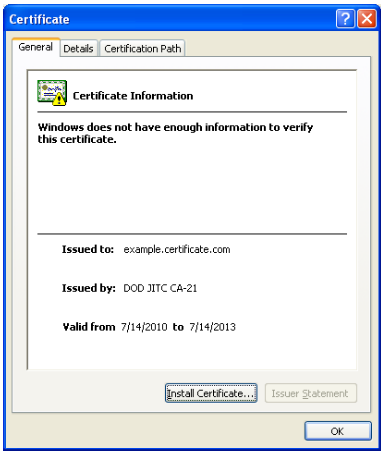
2.9 How Can I View Certificate Data Using the Windows Certificate Viewer?

To view certificate data encapsulated with "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" in the Microsoft Windows certificate viewer, follow these steps:

(These instructions were written based on Windows XP, but should be similar for other Windows variants.)

1.) Create a plaintext file (using the Windows Notepad or Wordpad applications, or equivalent)
2.) Copy the entire certificate, including the "`-----BEGIN CERTIFICATE-----`" and "`-----END CERTIFICATE-----`" lines into the file.
3.) Save the file as a plaintext file (not rich text, because rich text adds extraneous metadata to the file to denote fonts, styles, and formatting which interferes with the certificate data).
4.) On the desktop, change the extension from ".txt" to ".cer".
5.) Hit "Yes" when Windows prompts you to confirm the file extension change
6.) Double-click the file

You should see a window open similar to the following:



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: example.certificate.com

Issued by: DOD JITC CA-21

Valid from 7/14/2010 to 7/14/2013

2.10 How Can I Use OpenSSL To Validate and View Certificate Signing Requests?

Since the process of creating a certificate signing request can involve copying, pasting, and transferring the certificate signing request across different types of files and operating systems, it is possible to insert extraneous characters and spaces in the process. As result, when the certificate signing request finally reaches the DoD PKI to be signed, the certificate is rejected because the signature on the request no longer correctly computes. Tools like OpenSSL can be used to validate that the integrity of a certificate signing request is intact prior to its submission to the DoD PKI for signature. Some helpful commands are included in the following table:

(Note: Some environments may require approvals before OpenSSL software can be installed and executed.)

OpenSSL Command (Typed at the command prompt)	Function
openssl req -noout -text -in **<input CSR file>** Where <input CSR file> is the filename containing the certificate signing request to display	Allows one to view the details of the field values contained in the CSR.
openssl req -verify -noout -text -in **<input CSR file>** Where <input CSR file> is the filename containing the certificate signing request to display	Allows one to not only view, but verify the signature and integrity of the CSR. If the signature or file is not correct, an error message will appear. Otherwise "verify OK" will appear in the first line of the output on the screen, indicating that the CSR is intact.

2.11 What Do I Need to Tell My IT Staff to Allow Through Our Firewall?

OCSP and CRL requests transit the network using the HTTP protocol. As a result, firewalls and web-proxies may exist in your network that block the request for revocation information. In order to ensure that your system can successfully send OCSP and CRL requests (and receive the corresponding responses) you will need to submit an IT helpdesk ticket resembling the following:

Dear IT Helpdesk:

In order to allow our system **<insert UC system name>** to successfully send and receive OCSP and CRL request/responses, we require the following ports and IP addresses to be allowed through all web proxies and firewalls in the network as appropriate:

Outbound: Allow all unauthenticated HTTP traffic onto the WAN which has these characteristics:

1.) Source port: any, Source IP Address: **<Any IP address assigned to the UC system>**
2.) Destination port: 80, Source IP Address: Any of the following destination 8 IP addresses (corresponding to all known DoD OCSP responder sites and CRL distribution points):

    164.235.152.142
    164.235.104.142
    164.235.136.142
    164.235.72.142
    214.24.177.136
    207.133.227.104
    156.112.110.122
    156.112.102.122
    214.21.15.23 [Old IP Address -Not Valid after Sep 2011]
    152.229.242.172 [Old IP Address -Not Valid after Sep 2011]

Inbound: Allow all unauthenticated HTTP traffic from the WAN which has these characteristics:

1.) The HTTP session was originated from within the enclave
2.) Source port: 80, Source IP address: Any of the IP addresses listed above (the 8 OCSP and CRL IPs)
3.) Destination port: any (more specifically, the port used as the source port when the request was originated), Destination IP: The IP address within the UC system that originated the request.

2.12 Is There a Way To Request Certificates in Bulk?

The DoD PKI PMO has released a certificate enrollment tool called CRIMSON (Certificate Request Identity Management on Network) which may assist with requesting and retrieving large numbers of certificates. CRIMSON is a java-based application that uses a FIPS 140-2 validated cryptomodule to generate and submit certificates signing requests. CRIMSON and its associated documentation is available as free download from www.forge.mil. For more information, please use the following links:

http://iase.disa.mil/pki-pke/function_pages/tools.html
https://software.forge.mil/sf/go/proj1490

3 Acronyms

CA	Certificate Authority
CDP	Certificate Revocation List Distribution Point
CONUS	Continental United States
CML	Commercial
CN	Common Name
COTS	Commercial-Off-the-Shelf
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DISA	Defense Information Systems Agency
DNS	Domain Name Service
DoD	Department of Defense
DSN	Defense Switched Network
DTM	Delegated Trust Model
EKU	Extended Key Usage
EBC	Edge Boundary Controller
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
JITC	Joint Interoperability Test Command
KU	Key Usage
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
LSC	Local Session Controller
MILDEP	Military Department
NIST	National Institute of Standards
OCSP	Online Certificate Status Protocol
OS	Operating System
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standard
PKE	Public Key Enablement or Public Key Enabled
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-In User Service
RAE	Remote Ancillary Equipment
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman
SAN	Subject Alternative Name
SS	Softswitch
SSL	Secure Sockets Layer
TA	Trust Agent
TLS	Transport Layer Security
TNOSC	Theatre Network Operation and Security Center
UC	Unified Capabilities
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	United States
USMC	United States Marine Corp

VPN	Virtual Private Network
XP	Experience (as in Windows XP)

Appendix A: Troubleshooting Tips

The issues listed below reflect commonly encountered errors received on certificate request submission. (Special thanks to Navy SPAWAR and the DoD PKI PMO for providing these tips):

Issue: Sorry, your request is not submitted. The reason is "Invalid Request."
Solution: Resubmit the certificate request making sure there are no additional spaces before after the -----BEGIN CERTIFICATE----- or -----END CERTIFICATE----- tags. The system will attempt to read the leading or trailing blank spaces as part of the Base64 data and they cannot be interpreted.

Issue: Sorry, your request is not submitted. The reason is "Invalid Request."
Solution: Regenerate the CSR from the server making sure Key Usage (KU) and Extended Key Usage (EKU) fields are not populated erroneously by server defaults.

Issue: Sorry, your request is not submitted. The reason is "Rejected."
This message is received when the requestor is sending a 1024 request to a profile requiring a 2048 key (or the reverse) and does not satisfy the key-length constraint.
Solution: Submit CSR using correct key bit length for which the request was made.

The following issue is related specifically to CSRs made for Cisco equipment.
Issue: Sorry, your request is not submitted. The reason is "Invalid Request."
Solution: Resubmit the certificate request removing the begin and end tags (shown below) and making sure there is no leading or trailing white space:
-----BEGIN CERTIFICATE REQUEST-----
-----END CERTIFICATE REQUEST-----

Issue: The certificate is not accepted when loaded into the device or appears to be "corrupt."
Solution: When loading the certificate into equipment, try to do so in as direct a manner as possible. For example, avoid copying the certificate several times between different types of OSes, CDs, disks, etc. since this increases the chance that the certificate could become "corrupt" if even a single bit is altered. Also, be careful when opening and saving the certificate using word processing tools because some tools have been known to added in whitespaces and null characters that impact the processing of the certificate. Freely available tools like openssl can be used to validate the certificate and also compute the "digest" of the certificate file. If even one bit is altered in the file, the resulting digest will look completely different and will indicate if the certificate file was altered. (See Section 2.10 for more information.)

Appendix B: Example DoD PKI Action Item Register

This section provides an example action item register which can be used track all of the critical activities needed to request certificates for a given DoD PKI-enabled UC site. This example register assumes that external vendors or technicians will come on site to configure UC equipment, which requires that the certificates be ready, or close to ready, for installation when the technicians arrive. The anticipated steps reflect what should occur before, during, and after technicians arrive and should be incorporated into program tracking tools as appropriate.

Step	Checklist Item	Complete?
Items that should be completed before installers/techs arrive on site		
1.	Make sure that all equipment IP addresses and hostnames have been determined, especially for those products that require certificates. Ensure that the appropriate number of IP addresses have been requested for those devices that have multiple interfaces. If an IP addresses are planned for use in the “Subject” field of a certificate, ensure that this IP address is permanently assigned and will not change.	
2.	Ensure that all DNS and DHCP services are configured accordingly when Fully Qualified Domain Names (FQDNs) are planned for use in certificates such that the FQDN will resolve to the correct IP address.	
3.	Ensure that the implementers and PMs have all of the required IP address and FQDNs (hostnames) "in hand" prior to any technicians arriving on site.	
4.	Determine how many certificates need to be requested based on the number and type of equipment.	
5.	Call the LRA for the respective site to let them know the quantity of certificates that will be requested and ask what steps can be taken to expedite the certificate request. The LRA usually requires a form to be filled out when requesting certificates. Get a copy of this form at that time and get an example template illustrating how to fill out the form to minimize errors. LRA contact info is provided in Section 1.4 of this guide.	
6.	Ensure that the implementer or government POC on site has this LRA form "in hand" prior to any technicians arriving on site.	
Items to be completed on site (or before technicians arrive if possible) Proposed Completion Time for These Steps: **Within 24 - 48 hours**		
7.	Generate the certificate signing request for each device, following the equipment vendor instructions for generating the CSR or using a 3rd party tool if the device does not have the capability to generate its own CSR (see Section 1.2)	
8.	Copy the CSR from the equipment or tool and paste it onto the DoD PKI CA website following the steps in this guide (see Section 1.3) -- BE CAREFUL not to insert any extraneous characters or spaces when moving the CSR from the equipment to the DoD PKI CA during the CSR uploading process	
9.	Record the certificate request numbers returned after the cert has been uploaded (See Section 1.3.7)	
10.	Verify that “X” certificate request numbers are "in hand" by the PM for “X” numbers of certificates, where “X” is the number of requested certificates.	
11.	Complete the required LRA paperwork forms for each certificate request and submit the forms to the LRA. (see Section 1.4)	
12.	Call the LRA for a second time as soon as the CSRs are submitted and use the cert request numbers from step 9 to let them know that there are requests pending that need to be expedited. Use the LRA contact information provided in Section 1.4	

Step	Checklist Item	Complete?
13.	Turnaround should be within a few hours and at most the next day. If certificates are still not available, repeat step #12 and continue to call the LRA to make sure they approve the requests. Once the LRA approves, the DoD PKI should be able to issue the certificates within 20 minutes	
14.	Retrieve the certificates from the DoD PKI CA website following the instructions in this guide (Section 1.6) and load the certificates into the equipment. If any issues are encountered with the certificate, immediately call the LRA to discuss the problem and potential solution. Have the LRA verify that no problems existed with the CSR--otherwise the CSR would need to be regenerated.	
	After the Certificates Have Been Received	
15.	Note the expiration date of all of the issued certificates and all trust anchors (CA certificates)	
16.	Ensure that there is a documented procedure in place on site for how expiring certificates will be tracked over their 3 year (or less) lifetime. The plan should call for certificates to be replaced at least 60 days prior to their expiration. If certificate expire during operations, this will cause disruptions to operational telecommunications sessions and therefore must be avoided at all costs.	