

# Department of Health & Human Services Public Key Infrastructure (PKI) Program

## Common Policy TLS Certificate Request Procedures



Version 1.0 - DRAFT

July 2013

## 1. Document History

Date	Version	Author (s)	Description
<b>July 2013</b>	1.0	T. Gibbs C. Abruzzi B. Brown	Initial version. – Customized Entrust document for HHS – Added HHS-specific business process and PKI program information

## 2. Document Purpose & Scope

### 2.1 Purpose

This document is intended to provide an overview of HHS's PKI Program's Transport Layer Security (TLS) certificate offerings and to explain the steps for processing a Certificate Signing Request (CSR) for a Common Policy certificate.

### 2.2 Audience

There are three roles identified with the Common Policy TLS CSR process:

- System Owners/Administrators – are responsible for a system's (web server, database service) day-to-day operations and for generating CSRs for that that system
- Authorized Requestors – individuals authorized by their OpDivs to process CSRs on behalf of System Owners/Administrators
- Entrust Local Registration Authorities (LRAs) – persons trained and authorized by Entrust to approve CSRs for the Entrust CA

This document was written to provide Authorized Requestors, referred to as Requestors throughout this document, with the steps and information they need to successfully process CSRs on behalf of their OpDiv's System Owners/Administrators.

### 2.3 Scope

This document contains the procedures a Requestor will follow to process an HHS PKI Program's Common Policy TLS CSR. Public Trust processes vary slightly from the Common Policy request processes (e.g. User interface, URL etc.) and are considered out of scope for this document.

Additionally, the following information is out of scope for this document:

- Generating a CSR for a specific operating systems
- Installing a TLS certificate once it is retrieved by the requestor
- LRA training requirements and CSR approving procedures

### 3. HHS PKI Program’s TLS Certificate Overview

#### 3.1 Public Trust vs. Common Policy Based Certificates

The HHS PKI Program offers two different types of TLS certificates: Public Trust and Common Policy. The attributes of each type of TLS certificate is provided in the table below.

<b>PUBLIC TRUST</b>	<b>COMMON POLICY</b>
Also called “External TLS certificates” at HHS	Also called “Internal TLS certificates” at HHS
Trusted root CA is: <b>Entrust.net Certification Authority (2048)</b>	Trusted root is: <b>Entrust Managed Services Root CA</b>
Trusted root CA is widely distributed via the major internet browser vendors	Trusted root CA certificate must be distributed to relying parties and manually installed
Not cross-certified with the Federal Common Policy CA	Cross-certified with the <b>Federal Common Policy CA</b>

*\*Note: Instructions for Common Policy processes and procedures will be included as part of a separate user guide.*

In general, if a system or web server is going to be accessed only from within HHS, an Internal/ Common Policy TLS certificate is recommended. Because Common Policy TLS certificates are issued by HHS’s own CA, the CSRs are significantly less expensive than the Public Trust TLS certificates.

However, if a system or web server is going to be accessed by users/other systems external to HHS, a Public Trust TLS certificate is recommended.

### 4. HHS PKI Program Common Policy TLS Request Procedures

#### 4.1 Overview

The overall steps a Requestor will follow are:

1. Submit Common Name and Contact email address to the LRA
2. Access the HHS Entrust Enrollment Server for Web portal
3. Submit the CSR
4. Download the signed certificate

The remainder of this document explains in detail how to execute each of these steps.

## 4.2 Procedure for Requesting a Common Policy Certificate

Requestors should follow these steps for processing Common Policy CSRs on behalf of System Owners/Administrators.

### 3.2.1 Requesting and Receiving the Authorization and Reference Codes

The HHS Common Policy TLS CSR process begins with the Requestor sending an email to the HHS PKI Helpdesk. If approved, the email request will result in the receipt of two emails, each containing one piece of the Activation Code. One email will be received from the HHS PKI Helpdesk and the other email will be automatically generated by the Entrust HHS Enrollment Server for Web application. A Requestor will require both codes (Authorization code and Reference code) to generate a certificate request.

#### *Step 1:*

Send an email to the HHS PKI Helpdesk ([USHHSPKIHelpdesk@deloitte.com](mailto:USHHSPKIHelpdesk@deloitte.com)) containing the following information:

- The Common Name (CN) for the system/application requiring a certificate
- The Email address of the Authorized requestor.

Note: This email address will be used by the Entrust **HHS Enrollment Server for Web** application to send the Reference Code and will also be used to contact system administrators if and when Entrust notifications or certificate expiration notifications are required to be sent.

### 3.2.2 Submit a Certificate Signing Request (CSR)

The next step is to submit the certificate signing request (CSR), as generated by the requesting web server or other system, to the HHS Entrust Certificate Authority (CA) using the **HHS Entrust Enrollment Server for Web** application.

#### *Step 2:*

Log in to **Enrollment Server for Web** application by entering the following URL in your browser window:

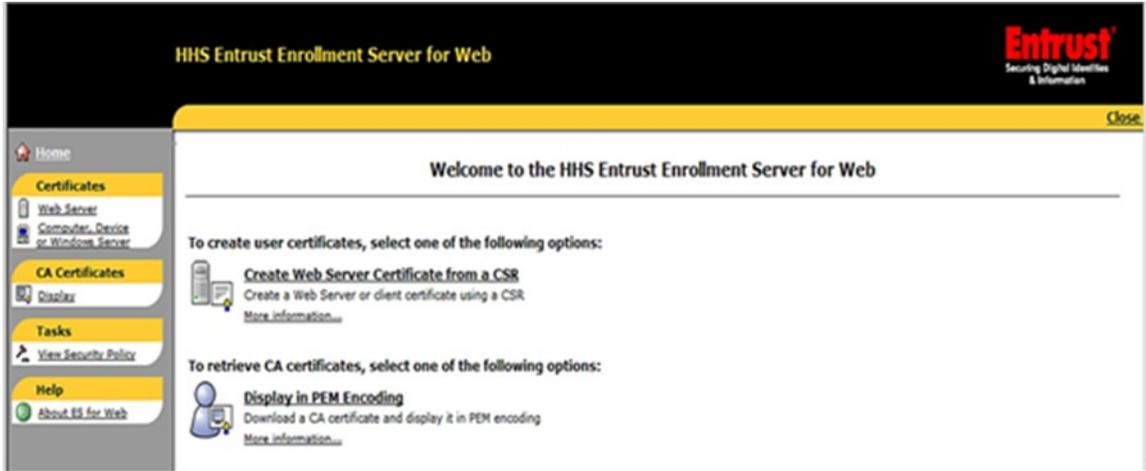
<https://hhspkienroll.managed.entrust.com/cda-cgi/clientcgi.exe?action=start>

This URL brings you to the HHS Entrust Enrollment Server for Web landing page.

**Step 3:**

From the landing page, click **Create Web Server Certificate from a CSR** from the main window, or click **Web Server** from the left hand menu.

Figure 1 HHS Entrust Enrollment Server for Web



The Web Server PKCS #10 Certificate Request form will appear.

Figure 2 Web Server PKCS #10 Certificate Request Form

The screenshot shows the "Web Server PKCS#10 Certificate Request" form. It features a title bar, a note stating "Note: here you can request a certificate for a Web Server or any client that supports PKCS#10 request.", and instructions: "In the fields below, enter the reference number and authorization code that you received from the Certification Authority. You can choose to view the certificate in raw DER format or in PKCS #7." Below this are input fields for "Reference Number:" and "Authorization Code:", and a dropdown menu for "Options:" currently set to "displayed as PEM encoding of certificate in raw DER". A large text area for the certificate request is provided, with instructions: "Please enter your certificate request (PKCS#10 request) in the following field. If you are requesting this certificate for a Web Server, make sure that your **Common Name (CN)** matches the **reference number** of the certificate being retrieved when generating the request. If you do not know how to generate this request, please consult your server documentation." At the bottom, there are "Submit Request" and "Reset" buttons.

**Step 4:**

Enter the **Reference number** and the **Authorization code** from the two emails you received (as noted in section 3.2.1 of this document).

**Step 5:**

From the Options drop-down list, choose the certificate format that is appropriate for the Web server platform that generated the CSR. The two options are:

- Raw Distinguished Encoding Rules (DER) format  
The DER format displays the certificate in raw text format.
- Public-Key Cryptographic Standard #7 (PKCS7).  
PKCS7 displays the certificate with mark-up tags.

**Step 6:**

Copy and paste the entire certificate request including the leading and post statements (e.g. **"Begin new certificate request"** and **"End new certificate request"**) into the large text box.

**Step 7:**

Click **Submit Request**.

The Entrust Managed Services CA signs the Web server certificate and sends it to Enrollment Server for Web.

**Step 8:**

Click **Download** on the page displaying your certificate and save the signed certificate to a location on your workstation where it can be easily located.

End of process.

For any questions regarding these HHS PKI Program Common Policy CSR procedures, or about the HHS PKI Program's TLS Certificate offerings, please send an email to: [USHHSPKIHelpdesk@Deloitte.com](mailto:USHHSPKIHelpdesk@Deloitte.com).