DO NOT PAY

helping **prevent** improper payments

Do Not Pay System Requirements and Reference Guide

System and Configuration Requirements

This document provides system and configuration for the online use of Do Not Pay.

Do Not Pay General Requirements

This section details the system and configuration requirements necessary to utilize Do Not Pay.

Operation System

The following operation systems are supported by Do Not Pay:

- ✓ Windows XP
- ✓ Windows 7

System Requirements

The following requirements are necessary to operate Do Not Pay:

- ✓ **Web Browser:** Internet Explorer 7.0 or 9.0
- ✓ **Entrust Root Certificate:** The Entrust (2048) Root Certificate must be installed in the "Trusted Root Certification Authorities" certificate store on the "local machine" (all user profiles) for the workstation. This certificate is normally installed by default with Internet Explorer. If it has been removed, you will need to have your agency reinstall the certificate.
- ✓ **Internet Options Security Settings**
- ✓ **Ports**
- ✓ **Windows Resolution:** 1280 x 1024 or higher

PKI Certificate Requirements

- ✓ **Login requires** PKI or PIV credentials
- ✓ Users must download software that will facilitate the use of their PKI Credential
  - Pentium II 500MHZ or Higher
  - 256 MB RAM
  - 100 MB Free Hard Disk space
  - One Free USB Port
  - 2X CD ROM Drive
  - Ability to download FMS PKI Installation software from FMS public website (https://itra.fms.treas.gov/fms_pki_installers.html). Full install download is approximately 70 MB
    - The PKI installation software contains:
      - o Smart card middleware
      - o Java JRE (Java runtime environment)
      - o JCE (Java cryptographic extensions) and certificate trust lists to be installed on agency workstation.

Hardware Requirements

- ✓ If your agency currently uses SafeNet to use and maintain a USB token you will not need to download the software required to use your PKI token.
- ✓ The iKey specifications can be found on the following web site: http://www.safenet-inc.com/library/edp/SafeNet_Product_Brief_iKey_2032.pdf.

  The iKey 2032 USB token has the following characteristics:
  - The iKey 2032 is a FIPS 140-2 Level 2 rated cryptographic module.

- The iKey 2032's NIST crypto module certification number is #161, last certified on 01/11/2007. The URL is: http://crsc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
- The iKey 2032 is not recognized as a USB storage module. It does not appear as a drive in Windows explorer. This means that the iKey is not prevented from being used if an agency defines its Windows Group Policy to write protect or disable USB ports. See Appendix B - USB Restrictions.

Software Requirements

Software is provided on a CD labeled **FMS PKI Setup** and is available at https://itra.fms.treas.gov/fms_pki_installers.html**.** The FMS PKI Setup CD should be provided to all end users during the FMS PKI enrollment process. The FMS PKI Setup CD will install all of components listed below. This setup will install and configure all needed components on the desktop to ensure successful operation of all FMS PKI applications. After successful installation of the FMS PKI Setup, agency end users will have the ability to access the following:

- ITRA – Credential creation and maintenance
- Any FMS PK enabled application the agency user is authorized to use.

Please contact your local support for any agency specific requirement (firewall/network config e.t.c).

For More Information

Email us at donotpay@stls.frb.org or call 1-855-837-4391.