z/OS V1R13

PKI services: Browser currency

Overview

- **Problem Statement / Need Addressed**
  - PKI Services support 2 types of browsers: Internet Explorer and Mozilla based browser.
  - Currently, PKI Services only support IE to use smart card for the Windows Logon certificate generation. Similar support is absent from the Mozilla based browser.
  - In IE, the PKI web pages use CAPICOM STORE APIs to allow the renewed certificate to be installed.
    - CAPICOM is needed to retrieve the original certificate so that the renew request can be regenerated, which is required when the renewed certificate is installed.
  - Although CAPICOM can still be installed in Windows 7, it is not supported. There is no guarantee that a Windows update will not stop its functionality.
- **Solution**
  - Enable the Mozilla base browsers on both the Windows and Linux platform to use the smart card to generate certificates.
  - Enable the IE browsers to use a homegrown .NET application (ActiveX) instead of CAPICOM for the installation of the renew certificates.
- **Benefit / Value**
  - This smart card enhancement is targeted at customers who want to request certificates from Mozilla based browsers which can run on both Windows and Linux.
  - The CAPICOM replacement is for customers who want to use Internet Explorer on Windows 7.

Usage and invocation

- For Smart Card Support in Mozilla based browsers
  - Once the smart card is installed in the PC, go to the Windows Logon template to request a certificate
- For using PKI Services ActiveX program to install renewed certificate
  - When you renew a certificate through an IE browser, if your PC does not have the Microsoft provided CAPICOM installed, you will be prompted to install this ActiveX program provided by PKI Services

Interactions and dependencies

- Software Dependencies
  - None if the customer chooses not to sign the ActiveX programs; otherwise he will need Microsoft signtool and Visual Studio to sign and re-package
- Hardware Dependencies
  - None
- Exploiters
  - PKI Services customers using Mozilla based browsers and IE browser running on a system without CAPICOM

Migration and coexistence considerations

- None

Installation

- For PKI administrator to set up the PKI Services ActiveX program for the customers download
  - If you choose to use the shipped ActiveX programs as they are:
    - Copy setup.exe and PKIXEnrollDeploy.msi from /usr/lpp/pkiserv/ActiveX/PKIXEnroll (for Windows XP and earlier end users)
    - Copy setup.exe and PKICEnrollDeploy.msi from /usr/lpp/pkiserv/ActiveX/PKICEnroll (for Windows Vista and later end users)
  - If you choose to sign the ActiveX programs first (recommended):
    - Get a code signing certificate to the PC
    - Copy the PKIXEnroll files from /usr/lpp/pkiserv/ActiveX/signsrc to the PC(for Windows XP and earlier end users)
    - Copy the PKICEnroll files from /usr/lpp/pkiserv/ActiveX/signsrc to the PC (for Windows Vista and later end users)
    - Use Microsoft Sign Tool to sign these shipped files to create the corresponding ActiveX programs
  - Update the Pass and Protect entries in the HTTP configuration files so that the user can access to these programs
- For PKI end user to install PKI Services ActiveX program in the PC using either way:
  - From the PKI Services home page
    - Click on the link
  - From the certificate renewal page
    - Click on the renew button

Appendix - References

- Publication references
  - PKI Services Guide and Reference (*SA22-7693*)
  - Security Server Command Language Reference *(SA22-7687)*