INSTALACIÓN DEL CERTIFICADO RAÍZ DE LA AUTORIDAD CERTIFICADORA UAEM

INDICE

Introducción

Para validar documentos PDF firmados electrónicamente es necesario indicar al software que se utiliza para este efecto la entidad o entidades en las que debe tener confianza.

La UAEM cuenta con su propia autoridad certificadora; Todos los certificados que se han emitidos están ligados a un certificado único denominado ***Certificado Raíz***, de forma tal que este acredita la identidad del titular del certificado emitido, ya que garantiza que la identidad del titular ha sido minuciosamente verificada. Por ejemplo, para el caso de individuos personalmente solicitando documentos originales, credenciales autorizadas con fotografía, verificando la fotografía con la persona, etc.

Este documento explica la forma de instalar el ***Certificado Raíz*** de la autoridad certificadora de la UAEM en el software de visualización de documentos PDF. Una vez hecho esto, por transitividad el software reconocerá automáticamente cualquiera de los miles de certificados emitidos por la autoridad certificadora UAEM.

Antes de aplicar el procedimiento de instalación del ***Certificado Raíz***, las firmas electrónicas incluidas en un documento PDF lucirán como en la siguiente imagen (que no representa una firma electrónica "verdadera"):

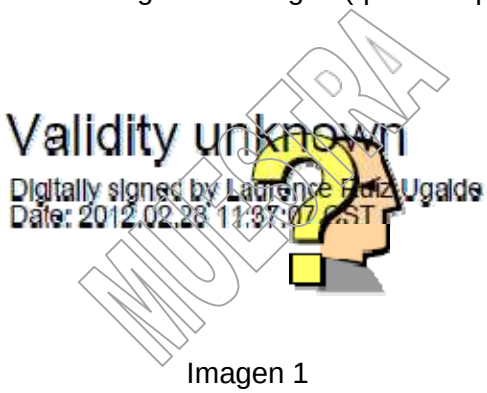

Imagen 1

Una vez aplicada la instalación del ***Certificado Raíz***, las firmas verificadas se verán como a continuación se muestra (que no representa una firma electrónica "verdadera"):

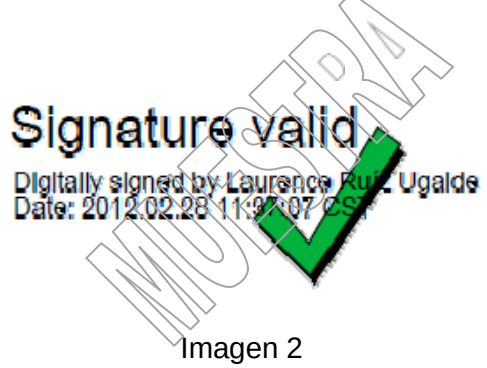

Imagen 2

Si al abrir un documento PDF que contiene firmas electrónicas y en el apartado correspondiente se visualiza la siguiente imagen (que no representa una firma electrónica "verdadera") lo cual indicara que el documento debe ser rechazado, puesto que su contenido ha sido alterado.

Imagen 3

Para conocer más detalles de la naturaleza el rechazo de la firma, podrá hacerlo seleccionando el área de la firma. La siguiente imagen muestra la forma en la que visualizara la información.

Imagen 4

Al final del presente documento, encontrará una firma "verdadera" del autor del mismo; con la cual podrá probar los procedimientos aquí indicados.

Instalación del certificado raíz de la autoridad certificadora UAEM

El siguiente procedimiento aplica al software visualizador de documentos PDF de la marca Adobe y funciona tanto para la versión sin costo (Adobe Reader), como para la versión comercial (Adobe Acrobat); por lo que debe tenerlo instalado previamente en su equipo de cómputo.

Es importante mencionar que este procedimiento ha sido verificado para los sistemas operativos: Microsoft Windows, Linux y MacOS.

Paso 1. Obtener el certificado raíz de la autoridad certificadora UAEM.
Este certificado, es un archivo que puede descargar desde varios medios de difusión masiva de la UAEM. Como por ejemplo, de su portal web.

Este paso no es necesario si ya cuenta con el archivo del certificado raíz. Es decir, porque se le haya proporcionado en un CD, una memoria, en un archivo procedente de un correo electrónico, por una descarga previa del archivo, etc.

Paso 2. Abrir el software de documentos PDF de Adobe (Adobe Reader o Adobe Acrobat).

Paso 3. Añadir el certificado raíz.
Para añadir el certificado raíz debe seleccionar la opción ***"Administrar identidades de confianza"***; que dependiendo el software visualizador (Adobe Reader o Adobe Acrobat) y la versión del mismo, puede encontrarse en una localización diferente, a la mostrada a continuación:

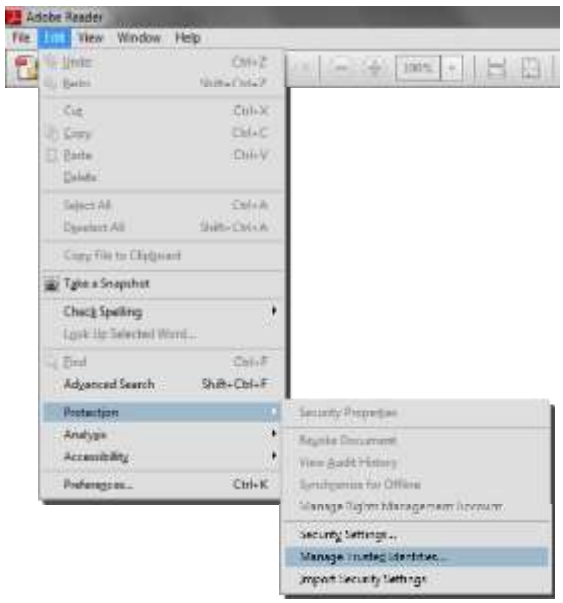

Imagen 5

Una vez seleccionada la opción de la Imagen 5 ("Gestión de Identidad de Confianza") se nos mostrará la siguiente pantalla en donde deberá seleccionar la opción "Certificados" en el apartado de "Desplegar" y posteriormente presionar el botón "Añadir contacto"

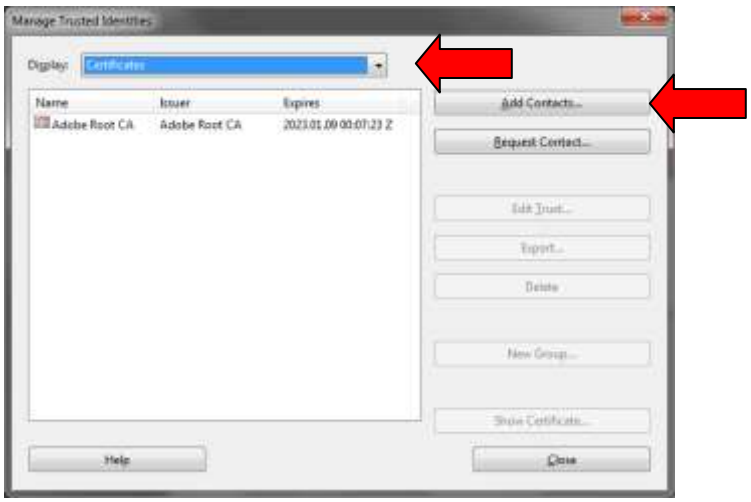

Imagen 6

De la pantalla mostrada presionar el botón "buscar…"

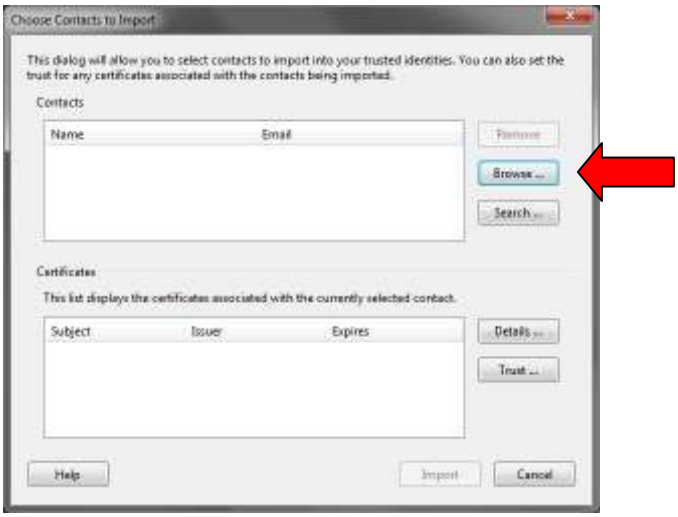

Imagen 7

Esto abrirá una ventana en donde seleccionará el archivo que contiene el certificado raíz de la autoridad certificadora UAEM.

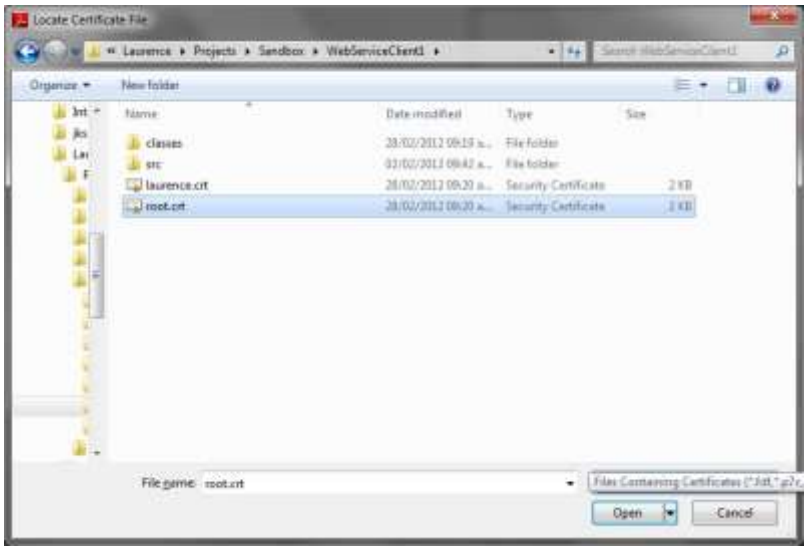

Imagen 8

Una vez seleccionado el archivo; se verá en la ventana anterior el contacto “Autoridad Certificadora UAEM” como se muestra en la siguiente imagen. Posteriormente deberá seleccionar haciéndo click con el ratón el certificado “Autoridad Certificadora UAEM” en la sección “Certificados”. Esta acción habilitará los botones rotulados “Detalles” y “Confianza”.

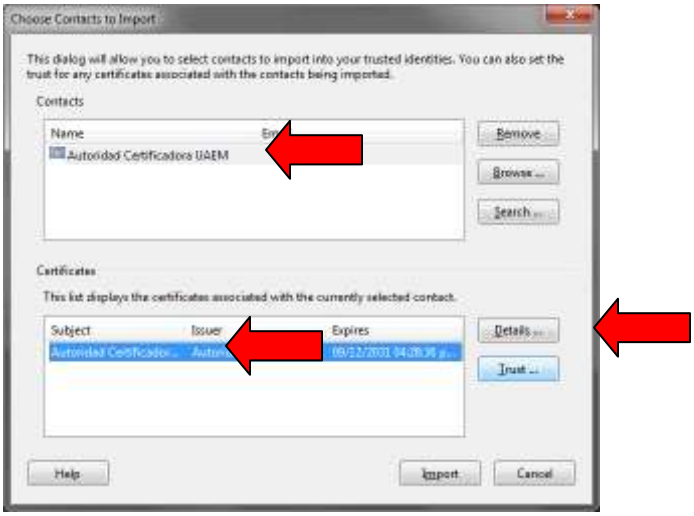

Imagen 9

Paso 4. Verificar el documento.

Para ilustrar mejor este paso se tomará como ejemplo la firma incluida al final del presente documento: Para determinar que este documento no es una versión alterada del original, debe ir al final del mismo y observar la firma electrónica, esta **NO** debe lucir como en la imagen 3, lo cual indicaría que el documento ha sido alterado; al contrario, esta debe lucir como en la imagen 1. En otro caso si luce como

en la imagen 2 significa que el certificado raíz ya ha sido instalado y no es necesario continuar con el procedimiento.

Paso 5. Verificar el certificado.

De la pantalla mostrada en la imagen 9 del paso 3, seleccionar el botón “Detalles”, lo que mostrará la ventana que se ilustra en la siguiente imagen. En esta, se tiene que seleccionar la pestaña rotulada como “Detalles” y posteriormente el renglón rotulado como “SHA1 digest”. El valor mostrado en la parte inferior de la misma **DEBE** ser el siguiente:

56 63 60 66 BB 4A 08 16 E8 3F A8 49 A3 A8 40 D8 11 52 0B C4

Si no fuera este valor, el certificado es falso y no debe proseguir con el proceso de instalación. Para regresar a la ventana anterior deberá seleccionar OK que se encuentra ubicada en la parte inferior derecha.

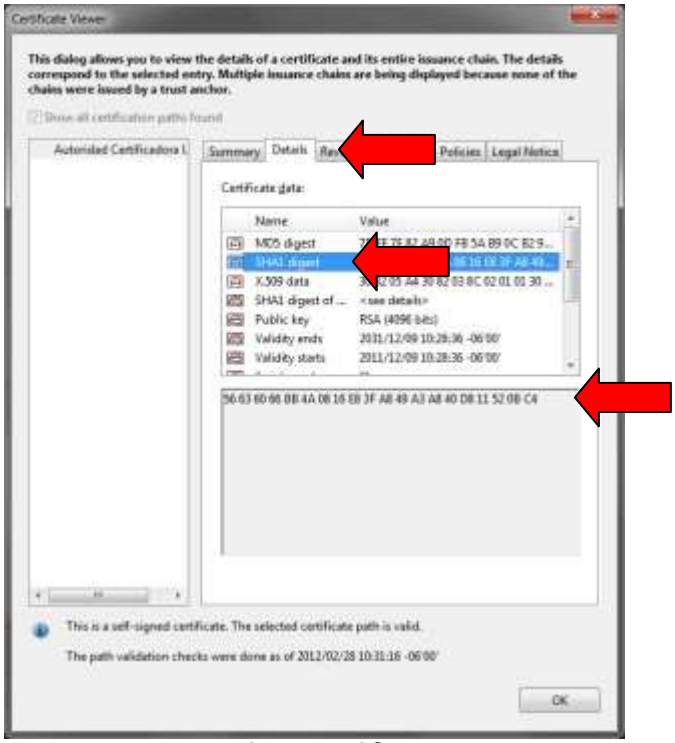

Imagen 10

Paso 6. Instalar el certificado raíz como "de confianza".

Para instalar el certificado de confianza deberá selccionar en la ventana mostrada el botón rotulado como "Confianza"

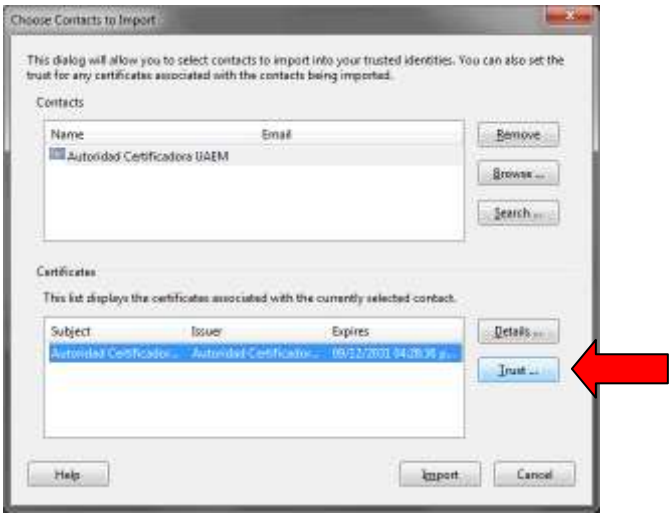

Imagen 11

Posteriormente seleccionar la opción "Utilizar este certificado como raíz de confianza" y presionar "Ok".

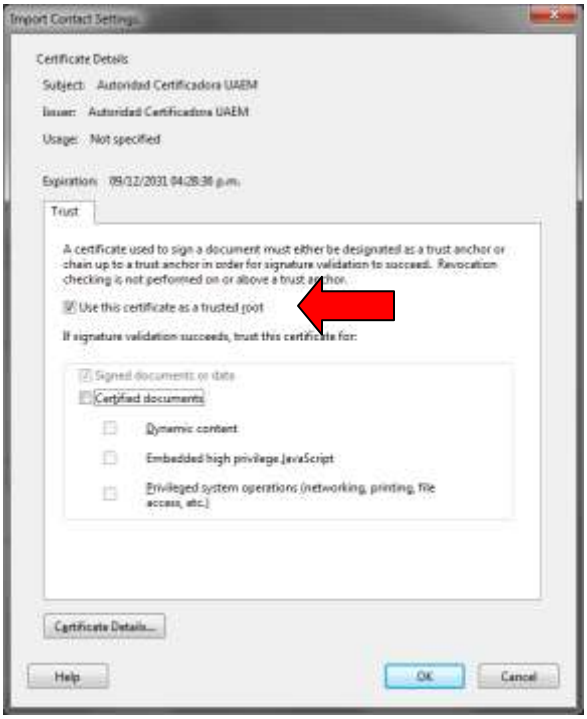

Imagen 12

Una vez hecho la anterior, en la ventana presionar el botón “Importar”

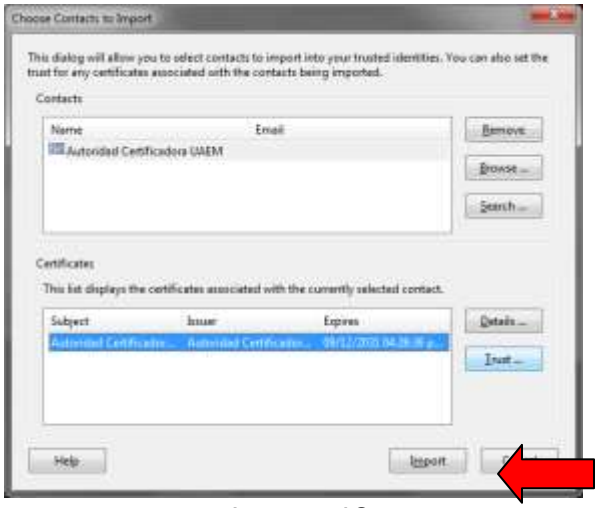

Imagen 13

Se confirmará la importación con una ventana similar a la siguiente:

Imagen 14

En la ventana de administración de identidades de confianza, se podrá ver el certificado de la autoridad certificadora UAEM. Seleccionar“Cerrar”.

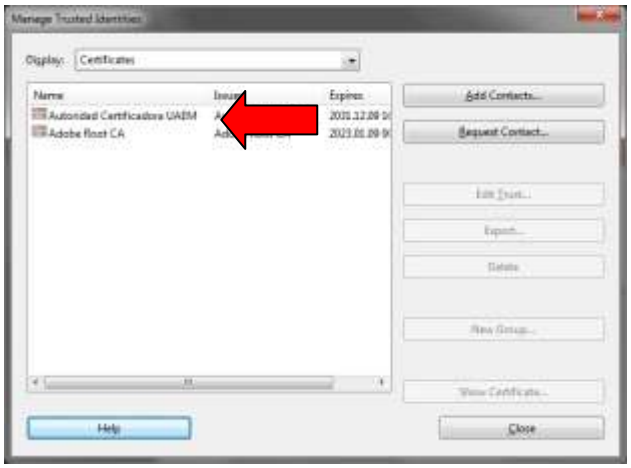

Imagen 15

Despúes de lo anterior, el certificado de la autoridad certificadora UAEM ya se encontrará instalado; por lo que si se llegara a tenere abierto algun documento PDF, no necesariamente será validado, solo bastará con indicar explícitamente la acción de validación de firmas, o cerrar el visualizador de archivos PDF y abrir nuevamente el documento.

Método alternativo a través del administrador de confianza de Windows

Este método sólo funciona en sistemas operativos Windows y es recomendable si además de ver documentos PDF firmados, se utilizan programas de Microsoft que requieren el uso de certificados digitales, emitidos por la autoridad certificadora UAEM. Como por ejemplo, sistemas de información en web propios de la UAEM, páginas seguras (en modo encriptado) visualizadas con el navegador de internet de Microsoft.

Procedimiento:

Paso 1. Obtener el certificado raíz de la autoridad certificadora UAEM

Paso 2. Abrir el certificado.
Para abrirlo será necesario dar doble clic en el archivo del certificado. La acción anterior mostrará una ventana como se ilustra en la siguiente imagen:

Imagen 16

Paso 3. Importar el certificado.

En el administrador de confianza de Windows (ver imegen 16), seleccione el botón “Instalar Certificado”, lo que nos mostrará la siguiente ventana en la cual tendra que seleccionar “Siguiente”.

Imagen 17

Posteriormente seleccione la opción “Colocar el certificado en el siguiente almacén” y despues “navegar” para seleccionar el certificado.

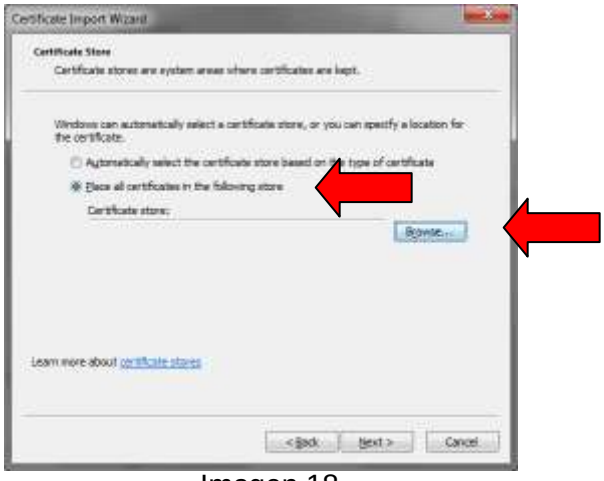

Imagen 18

De la ventana mostrada seleccione la opción “Autoridades certificadoras de confianza raíz” y oprimir “Ok”

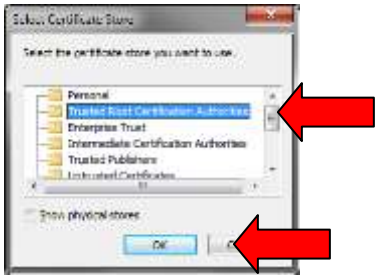

Imagen 19

Seleccione “Siguiente”

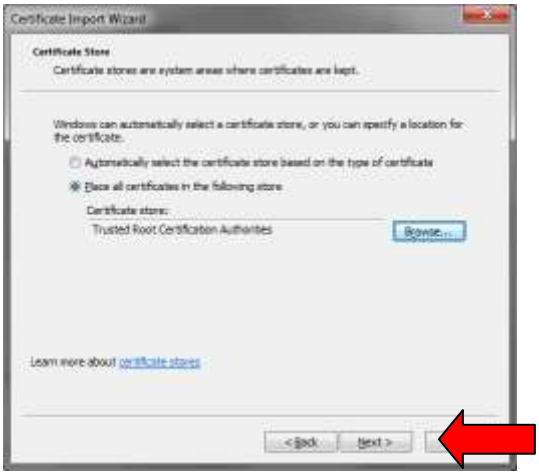

Imagen 20

Aquí tendra que selccionar “Finalizar”, para cerrar esta ventana.

Imagen 21

Paso 4. Verificar la huella digital del certificado

Una vez que se aseguró la autenticidad del certificado seleccionar “Si”. Como referencia véase el paso 4 y 5 de la sección anterior.

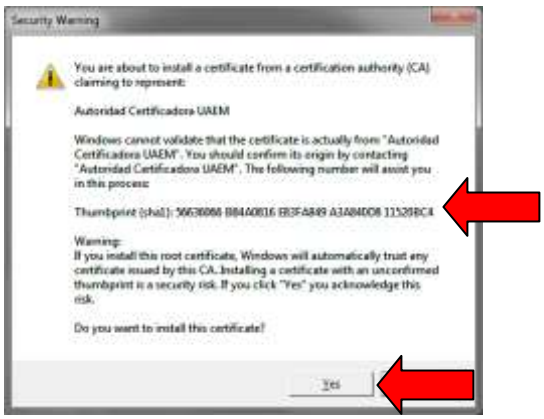

Imagen 22

Si no existe ningún problema con la importación, se le confirmará con un mensaje, similar a la ventana mostrada en la siguiente imagen. Prara cerrar la misma selccione “Ok”.

Imagen 23

Paso 5. Indicar al software de Adobe que confíe en los administradores de confianza de Windows.
Abrir el software visualizador de Adobe, y realizar lo siguiente: Seleccionar la opción “Preferencias”. Recordemos que como se mencionó anteriormente, dependiendo de la versión y si el visualizador es Adobe Reader o Adobe Acrobat, las opciones pueden encontrarse en una localización diferente a la mostrada a continuación:


Imagen 24

Lo anterior nos mostrará la ventana siguiente, en la cual tendrá que seleccionar la categoría “Seguridad” y posteriormente el botón rotulado como “Preferencias Avanzadas …”

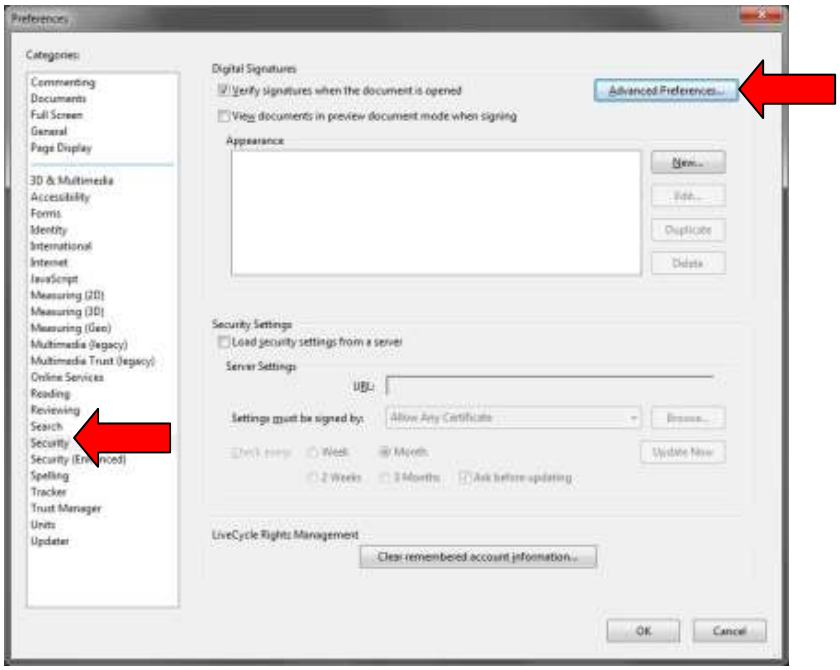

Imagen 25

En la ventana siguiente (imagen 26), seleccione la pestaña “Integración con Windows” y habilitar la opción “Búsqueda en los almacenes de certificados para certificados distintos a los suyos” y seleccionar “Ok”

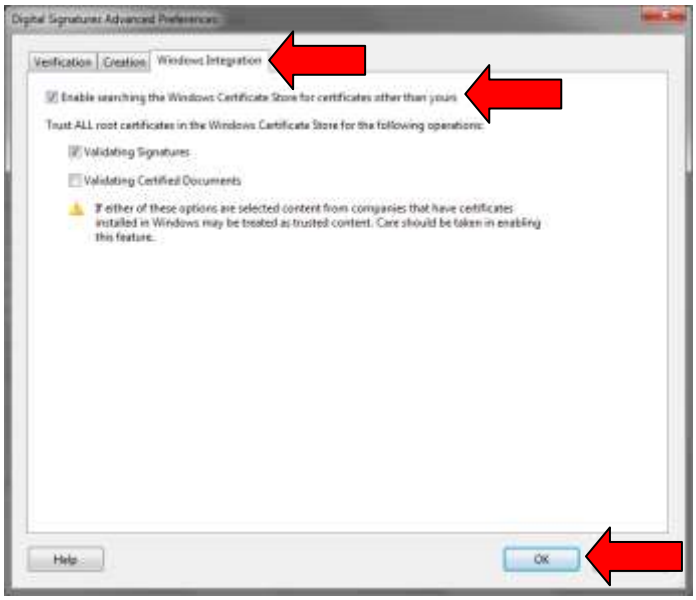

Imagen 26

Hecho lo anterior, seleccione “Ok” para cerrar la ventana activa.

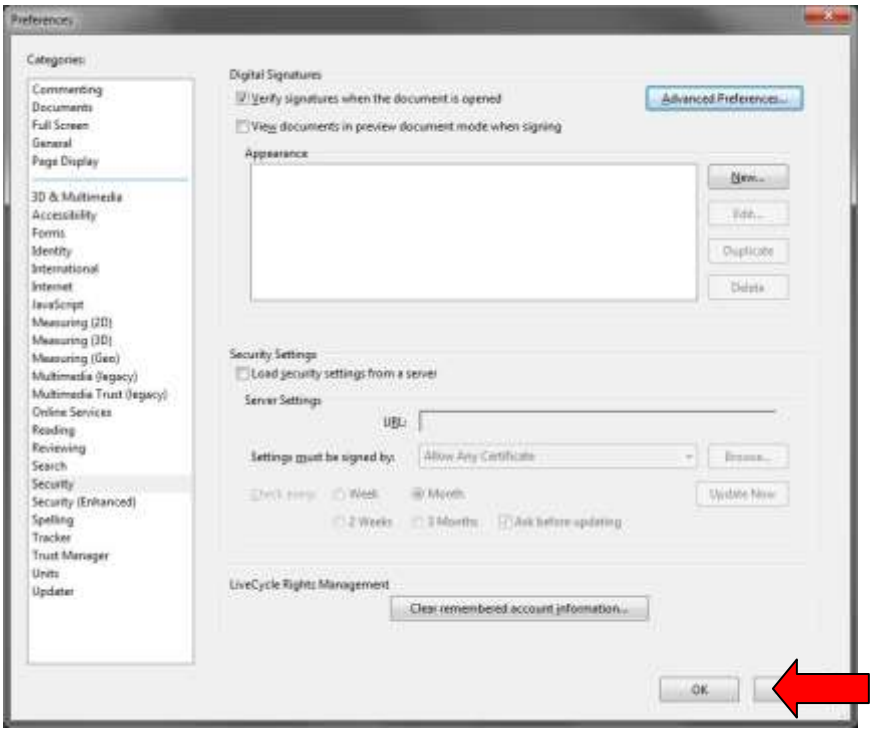

Imagen 27

Despúes de lo realizado anteriormente, el certificado de la autoridad certificadora UAEM ya se encuentra instalado; por lo si tiene abierto algun documento PDF no necesariamente será validado, solo bastará con indicar explícitamente la acción de validación de firmas, o cerrar el visualizador de archivos PDF y abrir nuevamente el documento.

Firma electrónica

Anexo I: Comité de Firmas y Sellos Electrónicos de la UAEM

Rectoría: Presidencia del Comité

Contraloría Universitaria: Validez de los procesos e implementación en sistemas de información

Dirección de Tecnologías de la Información: Infraestructura tecnológica, implementación en sistemas de información

Secretaría de Docencia: Implementación en sistemas de información

Dirección de Estudios Profesionales: Sistema de registro y validación de identidad, implementación en sistema de información PROED

Secretaría de Investigación: Implementación en sistemas de información

Abogado General: Aspectos legales

Dirección de Recursos Humanos: Proceso de registro y validación de identidad de empleados

Dirección de Recursos Financieros: Patrocinador, diseño arquitectónico, motor criptográfico, implementación en sistemas de información

Anexo II: Marcas, nombres y/o productos

Adobe, *Adobe Acrobat*, *Adobe Reader* y *Portable Document Format* (PDF) son marcas, nombres o productos registrados de *Adobe Systems Incorporated*.

Linux es marca, nombre o producto administrado por *The Linux Mark Institute*.

MacOS es marca, nombre o producto registrado de *Apple Inc*.

Microsoft, Microsoft Windows y Microsoft Internet Explorer son marcas, nombres o productos registrados de *Microsoft Corporation*.

Secure Hash Algorithm (SHA1) es publicado por el *National Institute of Standards and Technology*.