RED ELÉCTRICA
DE ESPAÑA

Guía de acceso a los sistemas e·sios

diciembre de 2016
Versión 1.2

Control de revisiones

Versión	Fecha	Modificaciones
1.0	02-10-2015	Versión inicial conjunta. Las anteriores guías de acceso de los diferentes sistemas se unifican en esta guía única.
1.1	4-12-2015	Modificados apartado de descarga e instalación de certificados de AC. Cambios editoriales.
1.2	16-12-2016	Eliminación de referencias a TLS 1.0 Eliminación de compatibilidad con algoritmo SHA-1 en firma digital. Eliminadas referencias a servicios web de WSDL específico. Ampliado el capítulo sobre los navegadores. Ampliado el capítulo de certificado cliente. Nuevo capítulo sobre la solicitud de soporte.

INDICE

1 Introducción

El presente documento desarrolla la guía de acceso a los sistemas e·sios. Se entiende por sistemas e·sios al conjunto de Sistemas de Información del Operador del sistema que incluyen entre otros: e·sios, e·sica, e·trans, Simel, GDE, Oficina EIC y Web Pública del OS.

2 Protocolos de acceso

El acceso a los sistemas e·sios se realizará mediante un canal seguro (https). En caso de que el sistema requiera de mecanismos de autorización / autenticación, se requerirá, de forma adicional, un certificado que identifique al cliente (2-way SSL).

En orden a garantizar la confidencialidad y seguridad de las comunicaciones solo se permite conectividad mediante los siguientes protocolos[1]:

- TLS v1.1
- TLS v1.2

Debido a que Windows XP, Windows Vista, Windows Server 2003 y Windows Server 2008 no soportan los protocolos antes mencionados, no será posible conectar con estos sistemas operativos.

Java soporta los protocolos TLS 1.1 y TLS 1.2 con un intercambio de claves superior a 1024 a partir de java 1.7 update 2[2]. Para evitar problemas de seguridad y rendimiento, recomendamos la última versión de java 1.8[3]

[1] SSL 2.0 es desaprobada en la RFC 6176. SSL 3.0 es desaprobada en la RFC 7568. Si bien TLS 1.0 no está explícitamente desaprobado, son muchas las compañías e instituciones que no recomiendan su uso: véase http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf y https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

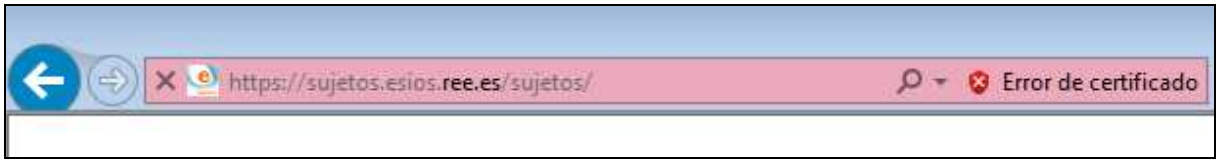
[2] https://docs.oracle.com/javase/7/docs/technotes/guides/security/enhancements-7.html

[3] Versiones antiguas de Java 1.7 y 1.8 no descargan los recursos desde webs que usan el protocolo TLS 1.2. Véase: https://bugs.openjdk.java.net/browse/JDK-8149914 y https://bugs.openjdk.java.net/browse/JDK-8065580

3 Certificado de AC

Debido a que la autoridad certificadora de los sistemas e·sios[4] no es reconocida por los navegadores, estos presentarán un mensaje de advertencia durante la conexión:

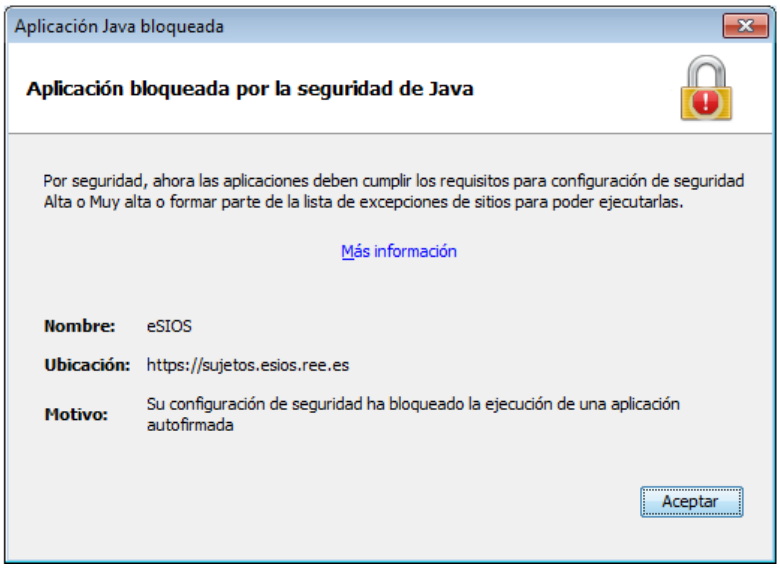
Si escogemos la opción de ir al sitio web, la aplicación funcionará sin problemas, pero mostrará una advertencia de seguridad en la barra de dirección:



La máquina java tiene un comportamiento similar. Si la aplicación web ejecuta applets, java nos informará que el sitio web no es de confianza:

[4] AC o CA Autoridad certificadora. "*Los certificados digitales serán emitidos por el OS actuando como Autoridad Certificadora. Los usuarios reconocen al OS como Autoridad Certificadora de confianza por el mero hecho de la utilización del certificado digital o tarjeta inteligente.*" P.O.-9 BOE-A-2012-10690

Bloqueando posteriormente la ejecución, incluso si se indica que se desea continuar:

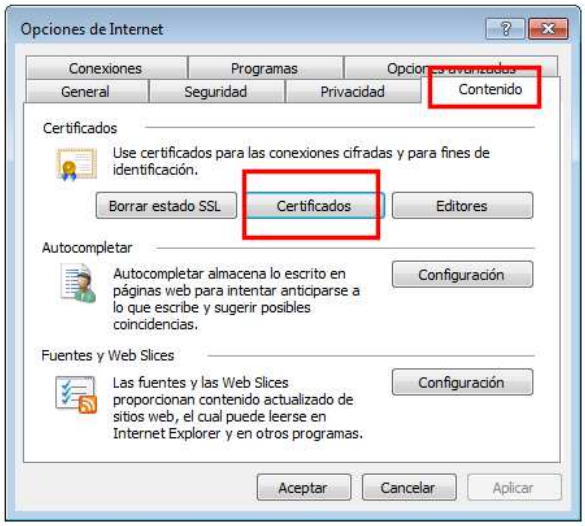


3.1.1 Obtención del certificado de AC

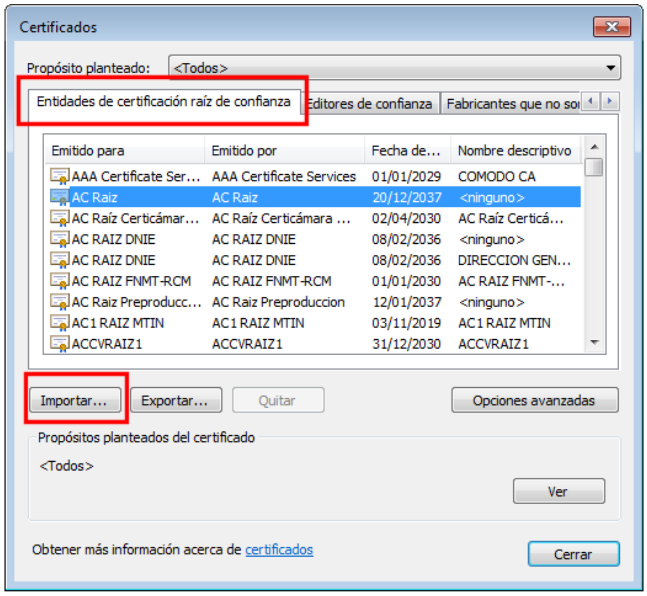
Para evitar los errores anteriores importaremos los certificados de la AC en el navegador y máquina java. Procederemos a descargar de la web https://pki.esios.ree.es el certificado raíz (`ac_raiz_ree.crt`) e intermedio (`ac_subordinada_ree.crt`)

3.1.2 Importación del certificado en el navegador

Internet Explorer escoja la opción "`Herramientas / Opciones de Internet`". En la pestaña "`Contenido`" haga clic sobre el botón "`Certificados`".



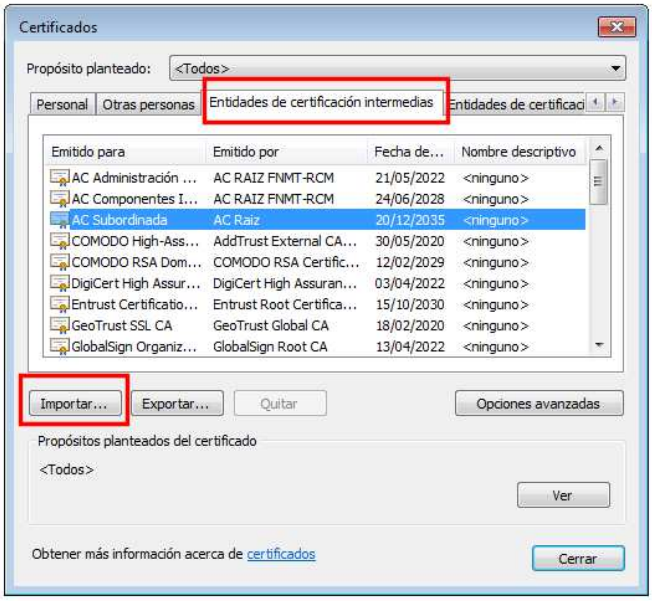
Escogeremos la pestaña "Entidades de certificación raíz de confianza" y pulsaremos el botón "Importar".



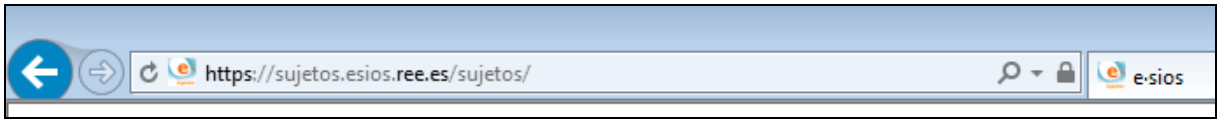
Se abrirá el asistente de importación de certificados. Avanzaremos por el asistente sin modificar ninguna opción. Cuando se solicite el archivo a importar indicaremos el archivo "ac_raiz_ree.crt" que hemos descargado anteriormente.

Continúe dejando todas las opciones del asistente por defecto. Cuando el asistente le muestre un diálogo de seguridad preguntado si desea instalar el certificado, conteste "Si".

Repetiremos la operación escogiendo ahora la pestaña "Entidades de certificación intermedias", haciendo uso del fichero "ac_subordinada_ree.crt"



Salga del navegador y vuelva a entrar. No debe aparecer ninguna página de advertencia y la barra de dirección ha de presentarse con fondo blanco:



3.1.3 Importación del certificado para uso en applets java[5]

Una vez importado el certificado de la CA en el navegador, no es preciso importar este en la máquina java para ejecutar los applets. De todos modos, recibiremos dos tipos de advertencias de seguridad:

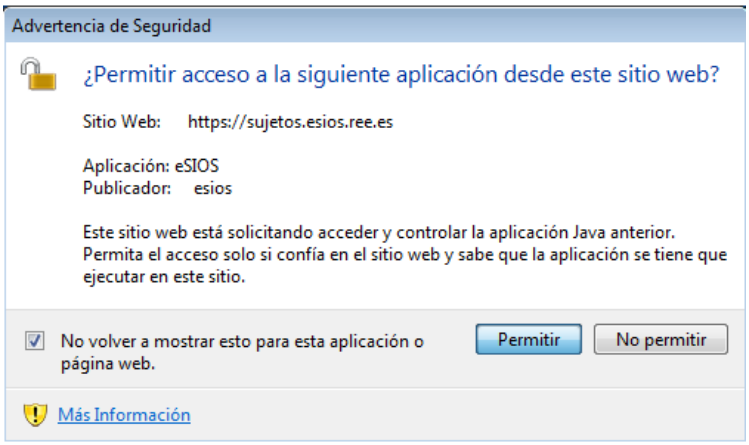
Una indicando que la página web ha cargado una aplicación sin accesos restringidos[6]. Proceda a marcar la casilla señalada en la imagen y pulse "`Ejecutar`"

Una segunda advertencia le indicará que el sitio web requiere comunicar información a la aplicación[7]. Marque la casilla y pulse "`Permitir`"

[5] El comportamiento indicado aplica a la versión 1.8.

[6] Las aplicaciones Java requieren de acceso a disco y acceso a los certificados de cliente para realizar las tareas de envío de mensajes por fichero y firma digital respectivamente.

[7] La página web utiliza los servicios que le proporcionan los applets, de ahí que exista esta doble comunicación.



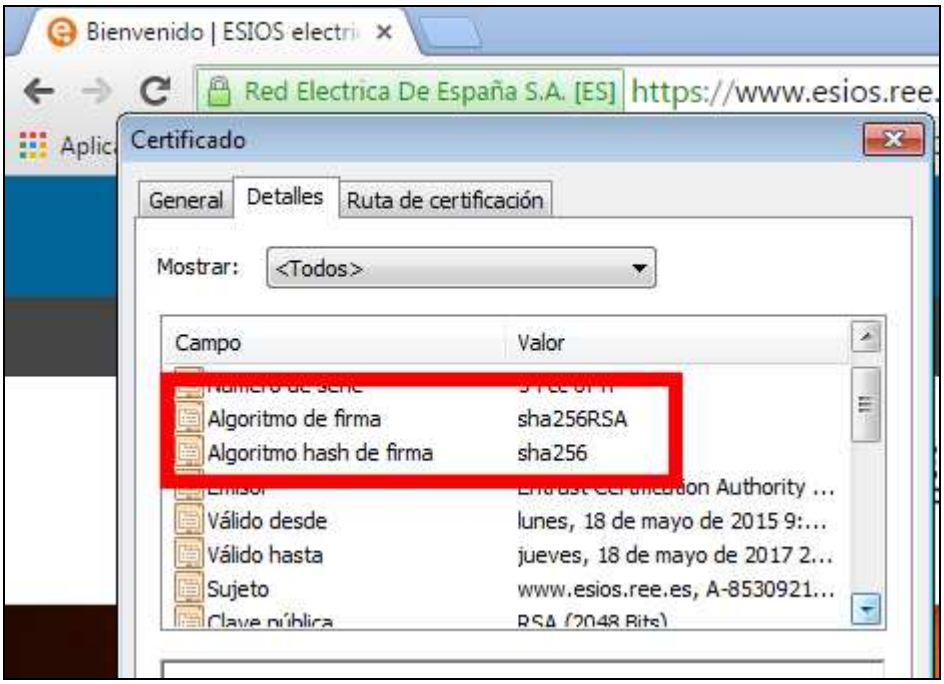
3.1.4 Importación de los certificados en el kit de conexión 62325-504

Para importar los certificados de la AC bastará con ejecutar la aplicación "`trustserver`". Consulte el manual de instalación y configuración del kit de conexión.

4 Certificado de servidor

Debido a los avances en computación, los certificados basados en el algoritmo SHA-1 han dejado de ser seguros. Navegadores y sistemas operativos dejarán de soportar SHA-1 en breve.

Los certificados SSL de los sistemas e·sios se emiten con el algoritmo SHA-2:



La compatibilidad de certificados SHA-2 es limitada en Sistemas operativos Windows XP y Windows Server 2003. Deberá revisar el nivel de actualización[8] de los mismos y hacer una prueba de conectividad.

Sistemas basados en OpenSSL deberán utilizar una versión superior a 0.9.8o

[8] https://support.microsoft.com/en-us/kb/938397

5 Certificado de cliente

Los sistemas e·sios requieren de certificado de cliente[9] para las tareas de autenticación (el sistema ha de conocer quién se conecta), autorización (el sistema decide qué acciones puede hacer el usuario conectado) y no repudio (firma digital).

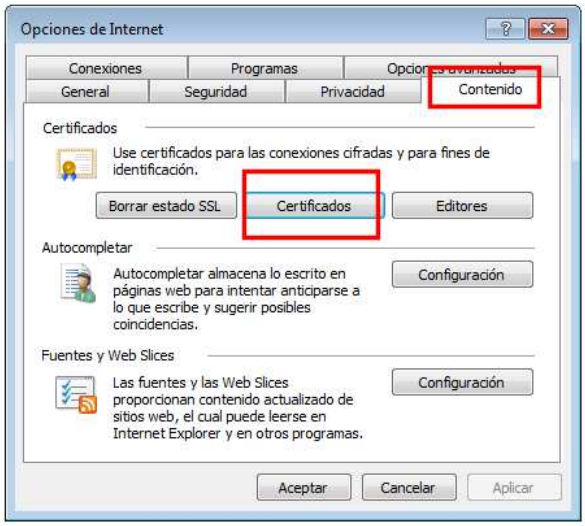
Los certificados cliente también se emiten usando algoritmo de firma SHA-2. Los usuarios que hagan uso de tarjetas inteligentes en lugar de fichero, deberán comprobar que su lector es compatible con SHA-2. Red Eléctrica de España no provee de tarjetas ni de dispositivo lector.

5.1 Instalación de certificado de cliente

El certificado cliente se descargará desde la web de PKI, tras haber recibido un correo con las claves de descarga.

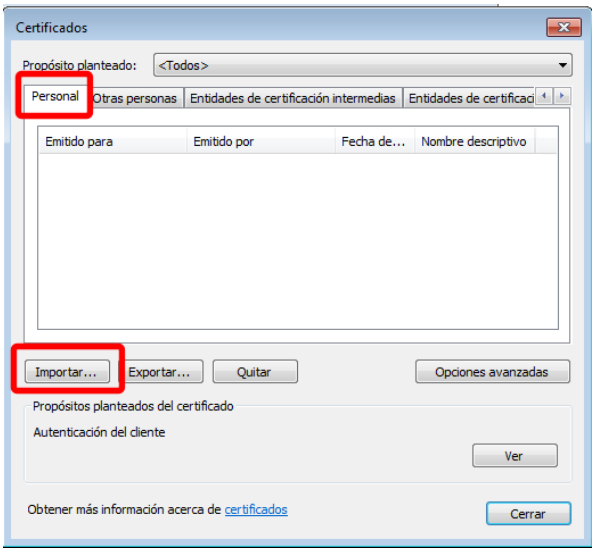
IMPORTANTE: Una vez descargado el certificado, este no se puede volver a descargar. Tenga especial cuidado al escoger la contraseña para evitar que este quede inservible. Red Eléctrica de España no conoce las contraseñas escogidas por los usuarios ni tiene acceso a los certificados por ellos descargados.

Para importar el certificado, en Internet Explorer escoja la opción "`Herramientas / Opciones de Internet`". En la pestaña "`Contenido`" haga clic sobre el botón "`Certificados`".



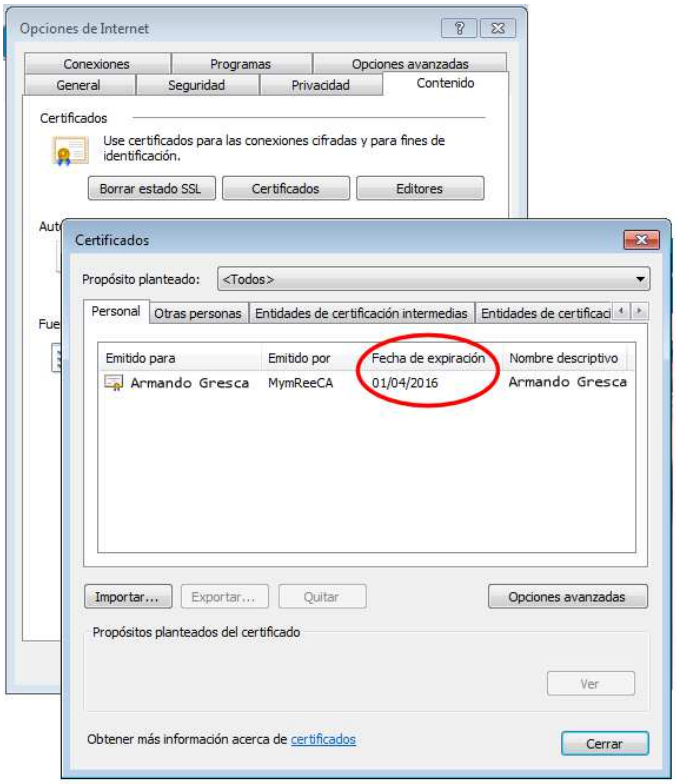
Escoja la primera pestaña "`Personal`" y pulse el botón "`Importar`":

[9] Consúltese BOE-A-2012-10690 P.O-9



El asistente le preguntará la ruta del archivo de certificado y la contraseña de este.

Los certificados digitales se emiten con fecha de caducidad. Es responsabilidad del usuario solicitar la renovación del certificado con antelación suficiente. Puede consultar la fecha de caducidad de su certificado utilizando la opción de Internet Explorer "`Contenido`" / "`Certificados`"



Los certificados basados en SHA-1 seguirán siendo válidos hasta la fecha de caducidad de los mismos.

Red Eléctrica de España se reserva el derecho de revocar -sin previo aviso- un certificado de cliente si observa que este es utilizado de forma incorrecta. Se considera que un usuario hace un uso inadecuado si realiza, entre otras acciones:

- Búsqueda de vulnerabilidades, intentos de inyección de código, intentos de ejecución de scripting, etc.
- Intentos de acceso a datos de terceros, envío de información para un titular no representado, solicitud de mensajes de terceros, etc.
- Solicitudes reiteradas de mensajes inexistentes.
- Envíos de mensajes sobre los cuales no se tiene un rol adecuado o envío de mensajes salientes.
- Peticiones por servicios web que violan los límites establecidos –y que deben ser conocidos- como por ejemplo listados que comprenden más del número de días especificados, uso de filtros con valores fuera de rango (versiones mayores de 999 por ejemplo) realizar más solicitudes por minuto de las posibles, etc.

El titular del certificado es responsable a todos los efectos de este mal uso, incluso si el certificado ha sido cedido a terceros para la explotación del sistema.

La compañía del usuario que realice este tipo de prácticas perderá la capacitación técnica.

6 Firma digital

El no-repudio de la información intercambiada se logra mediante la firma digital de los documentos. La firma se implementa haciendo uso de XML signature[10]

Al igual que se ha comentado anteriormente, los algoritmos SHA-1 también están desaconsejados tanto en las tareas de obtención del hash (digest) como en la firma propiamente dicha debiéndose utilizar el algoritmo SHA-2 en ambos casos.

Cabecera de una firma con algoritmo SHA-2:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <Reference URI="">
          <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <DigestValue>. . .
```

[10] http://www.w3.org/TR/xmldsig-core1/

7 Máquina Virtual Java

Los applets de las aplicaciones web requieren de una versión de java 1.7 o superior. Dado que desde abril del 2015 la máquina java 1.7 no está soportada por Oracle[11], le recomendamos haga uso de la versión 1.8[12].

No es preciso modificar los valores de seguridad -o cualquier otra opción- de la máquina java. Tenga en cuenta que si modifica la máquina java, no podremos darle soporte (véase el apartado 10)

8 Navegador

Las aplicaciones web que hagan uso de applets requieren de Microsoft Internet Explorer 11.

Google Chrome no soporta la ejecución de java (applets).

La web de sujetos de e·sios requiere la vista de compatibilidad para su funcionamiento. Puede incluir la URL de la web de sujetos en la vista de compatibilidad mediante la opción "`Configuración de Vista de compatibilidad`" que aparece en el menú de herramientas de Internet Explorer.

La web de la PKI no funcionará de forma adecuada si está incluida en la vista de compatibilidad. Utilice otro navegador distinto a Internet Explorer para descargar los certificados o bien elimine el sitio web de la configuración de Vista de compatibilidad.

9 Servicios web

Los sistemas e·sios ofrecen una interfaz web services basada en la especificación técnica IEC 62325-504. Para facilitar las tareas de desarrollo de clientes basados en esta interfaz, hay disponible una implementación de código abierto que puede ser accedida desde la siguiente dirección: https://bitbucket.org/smree/

Consulte el área de descargas disponible en: https://bitbucket.org/smree/eemws-core/downloads

10 Solicitando soporte

Puede solicitar soporte enviando un correo electrónico a la dirección: soportesios@ree.es

Para evitar ser respondido de forma inmediata con un nuevo correo solicitándole más información, les rogamos indiquen en su consulta:

- URL completa de la aplicación web de la que se solicita soporte.
- Código del certificado de usuario utilizado (si procede).
- Captura de pantalla **legible** donde se muestre el error.
- Descripción del error (datos de entrada, opción del menú utilizada, etc.)
- Fecha y hora en la que se produce el error.
- Versión de navegador.
- Versión de máquina java.

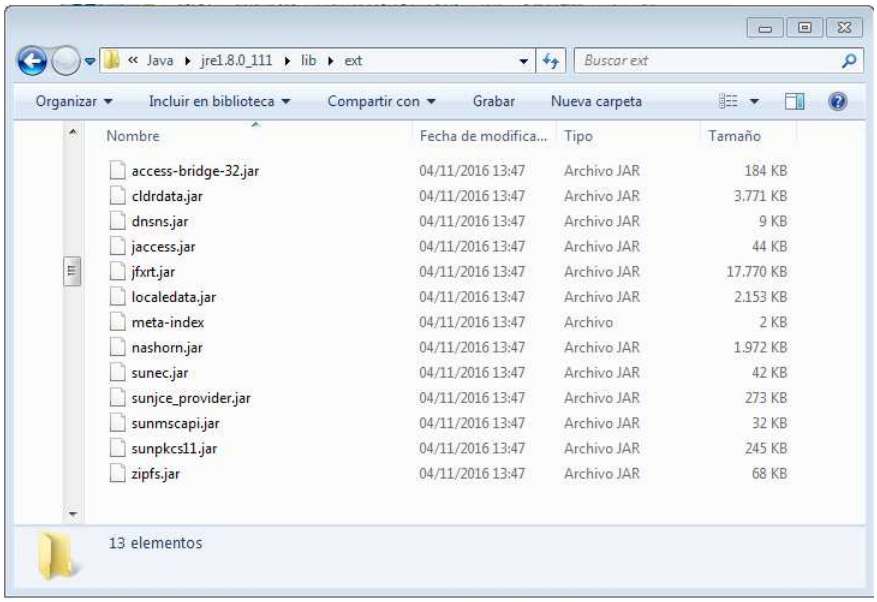
[11] http://www.oracle.com/technetwork/java/eol-135779.html

[12] Versiones antiguas de Java no descargan los recursos desde webs que usan el protocolo TLS 1.2. Véase: https://bugs.openjdk.java.net/browse/JDK-8149914 y https://bugs.openjdk.java.net/browse/JDK-8065580

10.1 Problemas con la máquina java (applets)

En caso de tener problemas en la carga y ejecución de applets, compruebe primero si su máquina java ha sido modificada. Para ello remítanos una captura de pantalla con la lista de ficheros existente en la carpeta de extensiones de java. Por ejemplo para java 1.8.0 rev 111 la ruta sería[13]:

```
C:\Program Files (x86)\Java\jre1.8.0_111\lib\ext
```



Las librerías del directorio de extensiones están disponibles para cualquier aplicación java que se ejecute en su equipo, sin importar el origen de la misma (un applet sea cual fuere la página donde está embebida o una aplicación de escritorio). Si estas librerías de terceros sobre-escriben librerías de la distribución estándar de java (especialmente las de seguridad) todo su sistema se verá comprometido.

Importante: No damos soporte a configuraciones que presenten librerías de terceros adicionales a las de la distribución estándar de java. No podemos dar soporte a elementos que no conocemos.

Para remitir una copia de la salida de su máquina java sigua los siguientes pasos:

1.- Abra el panel de control de Windows.

2.- Dentro del panel de control, abra ahora el panel de control de java

3.- En la ventana "Avanzado" busque la categoría "Consola de Java" y marque dentro de esta "Ver Consola".

4.- Salga del panel de control y entre en la aplicación.

5.- Deberá aparecer una ventana adicional: La consola de java. Haga click sobre esta ventana y pulse el número "5" en el teclado (no use el teclado numérico). Aparecerá un texto indicando que se ha activado el modo de depuración.

6.- Recargue la aplicación y repita los pasos que producen el error.

[13] Si tiene dos instalaciones de java para 32b y 64b, compruebe la versión que es utilizada por su navegador.

7.- En la consola de java, pulse el botón inferior “Copiar” y pegue el contenido en su cliente de correo.

10.2 Problemas con los servicios web

Solo se proporcionará soporte al cliente de servicios web disponible en la web de bitbucket (https://bitbucket.org/smree/) y siempre y cuando este no haya sido modificado incluyendo librerías de terceros u otras modificaciones.

Si su cliente de servicios web presenta algún problema, debe dirigirse a la empresa suministradora del mismo en primera instancia. No podemos dar soporte a un software que desconocemos.

10.3 Problemas y consultas reportados por terceros

En caso de que la consulta sea realizada por una empresa colaboradora de un sujeto / participante / agente (típicamente la empresa IT contratada por este) el correo de consulta ha de tener **obligatoriamente** en copia, al menos, un contacto reconocido (y no externo) de la empresa por la cual se consulta.