

Configurando SSL/TLS

Hacia la seguridad real...

Miguel Macías Enguïdanos
miguel.macias@upv.es



Red
IRIS



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

XXXIV Grupos de Trabajo
Bilbao, 27/11/2012

Índice

- Introducción
- Ejemplos actuales
- Opinión generalizada
- Situación ideal
 - confidencialidad
 - integridad
 - disponibilidad
 - autenticidad
- La web: un caso especial

Esquema Nacional de Seguridad

- ENS (Real Decreto 3/2010)

- Preámbulo

*La finalidad del Esquema Nacional de Seguridad es la **creación de las condiciones necesarias de confianza** en el uso de los medios electrónicos, a través de **medidas para garantizar la seguridad de los sistemas**, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.*

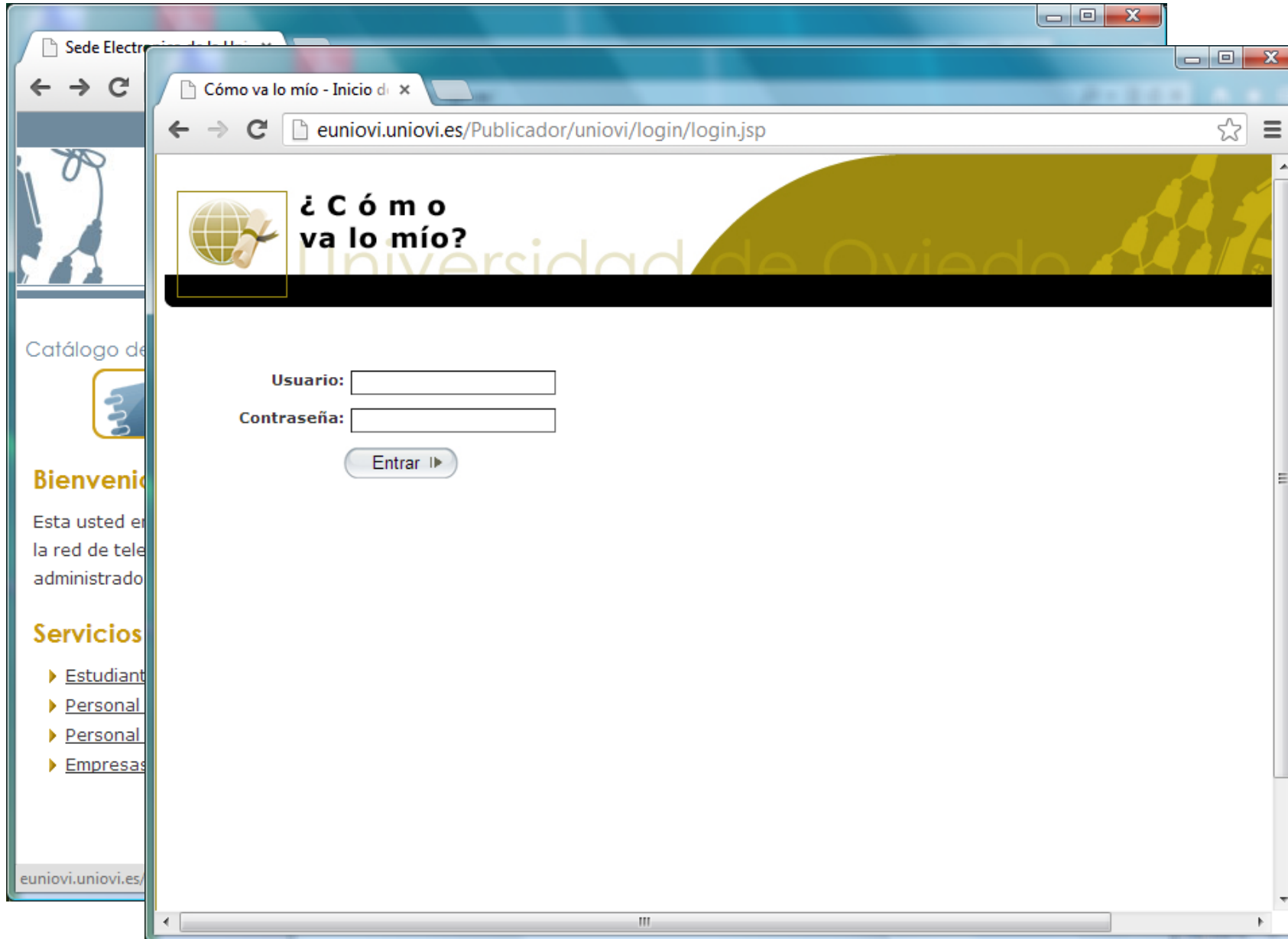
Estado actual

- De todos los cambios que implica el ENS, puede parecerse que la parte más sencilla es asegurar las comunicaciones
- **SSL/TLS** es sencillo de implementar en cualquier sistema y, de hecho, es algo que ya tenemos (prácticamente) todos en marcha
- Incluso la mayoría de usuarios reconocen el uso de SSL y lo “exigen” (en algunos servicios, al menos)
- ¿Podemos estar tranquilos? ¿lo hacemos bien?
¿estamos generando confianza? ¿mejor tener SSL, sea como sea, que no tener nada?

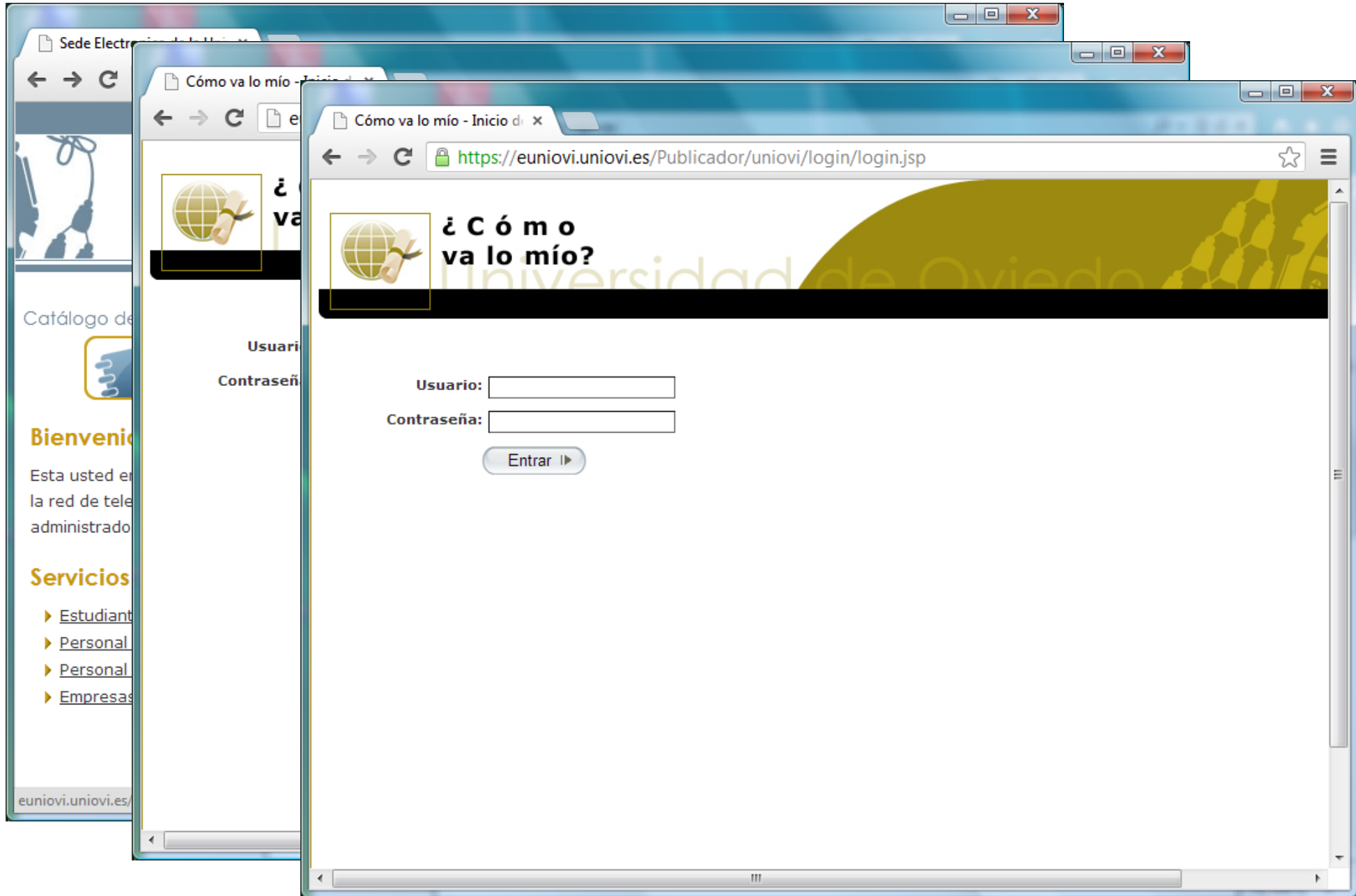
Ejemplo 1: sin seguridad (1/3)

The screenshot shows a web browser window with the address bar displaying <https://sede.uniovi.es>. The browser's address bar and the page's content area both show the text "https://sede.uniovi.es", which is a significant security indicator error. The website header includes the title "Sede Electrónica Universidad de Oviedo" and navigation links for "Mapa web", "Contacto", and "Buzón de correo". The main content area features a "Bienvenido/a" message, a "Servicios electrónicos" section with links for "Estudiantes", "Personal de administración y servicios", "Personal docente e investigador", and "Empresas e instituciones", and a "Destacados" section with links for "Carta de Servicios electrónicos", "Preguntas frecuentes", "Recomendaciones de navegación", and "Normativa". A sidebar on the right contains a date and time display ("23 noviembre de 20:42:44 C") and a list of links including "Sobre la Sede", "Tablón de Anuncios", "Fecha y Hora", "Calendario", "Ayuda", and "Enlaces". The footer of the browser window shows the URL "euniovi.uniovi.es/Publicador".

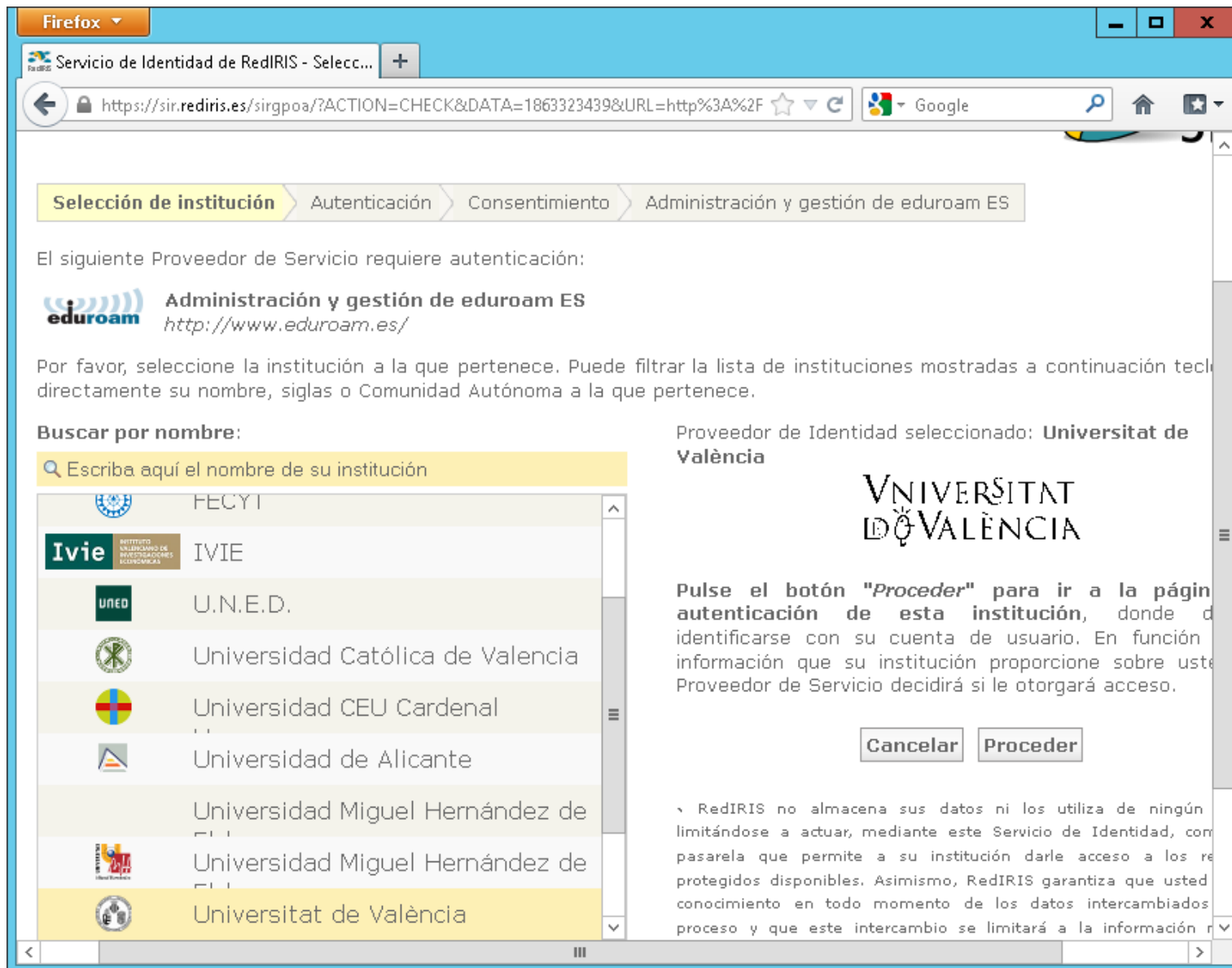
Ejemplo 1: sin seguridad (2/3)



Ejemplo 1: sin seguridad (3/3)



Ejemplo 2: sin seguridad (1/3)



Firefox


Servicio de Identidad de RedIRIS - Selecc... +

https://sir.rediris.es/sirgpoa/?ACTION=CHECK&DATA=1863323439&URL=http%3A%2F

Google

Selección de institución Autenticación Consentimiento Administración y gestión de eduroam ES










El siguiente Proveedor de Servicio requiere autenticación:

 **Administración y gestión de eduroam ES**
<http://www.eduroam.es/>


Por favor, seleccione la institución a la que pertenece. Puede filtrar la lista de instituciones mostradas a continuación tecleando directamente su nombre, siglas o Comunidad Autónoma a la que pertenece.

Buscar por nombre:

Escriba aquí el nombre de su institución

	FECYT
	IVIE
	U.N.E.D.
	Universidad Católica de Valencia
	Universidad CEU Cardenal
	Universidad de Alicante
	Universidad Miguel Hernández de Alicante
	Universidad Miguel Hernández de Elche
	Universitat de València

Proveedor de Identidad seleccionado: **Universitat de València**



Pulse el botón "Proceder" para ir a la página de autenticación de esta institución, donde deberá identificarse con su cuenta de usuario. En función de la información que su institución proporcione sobre usted, el Proveedor de Servicio decidirá si le otorgará acceso.

Cancelar Proceder

RedIRIS no almacena sus datos ni los utiliza de ningún modo, limitándose a actuar, mediante este Servicio de Identidad, como pasarela que permite a su institución darle acceso a los recursos protegidos disponibles. Asimismo, RedIRIS garantiza que usted tiene conocimiento en todo momento de los datos intercambiados en este proceso y que este intercambio se limitará a la información necesaria para la autenticación.

Ejemplo 2: sin seguridad (2/3)

The screenshot shows a Firefox browser window with two tabs. The active tab is displaying a page from <https://sir.rediris.es/sirgpoa/?ACTION=CHECK&DATA=1863323439&URL=http%3A%2F>. The page content includes a navigation bar with 'Selección de institución', 'Autenticación', 'Consentimiento', and 'Administración y gestión de eduroam ES'. Below this, it states 'El siguiente Proveedor de Servicio requiere autenticación:' and lists 'Administración y gestión de eduroam ES' with the URL <http://www.eduroam.es/>. A list of institutions is visible, including 'Universidad Católica de Valencia', 'Universidad CEU Cardenal', 'Universidad de Alicante', 'Universidad Miguel Hernández de', and 'Universitat de València'. A modal dialog box titled 'Identificación requerida' is overlaid on the page. The dialog contains the text: 'http://uvpapi.uv.es está solicitando un nombre de usuario y una contraseña. El sitio dice: "LDAP Auth"'. It has two input fields: 'Nombre de usuario:' and 'Contraseña:'. Below the fields are 'Aceptar' and 'Cancelar' buttons. The status bar at the bottom of the browser shows 'Esperando a uvpapi.uv.es...'. The background page also has a 'Cancelar' and 'Proceder' button at the bottom.

Ejemplo 2: sin seguridad (3/3)

The screenshot shows a Firefox browser window with a security warning dialog box. The warning is titled "Conexión no confiable" (Unreliable connection) and states: "Esta conexión no está verificada" (This connection is not verified). It explains that Firefox was asked to connect securely to uvpapi.uv.es, but the connection cannot be confirmed as secure. The dialog also provides technical details: uvpapi.uv.es uses an invalid security certificate, and the certificate is only valid for mmedia.uv.es. The error code is sec_error_unknown_issuer. A button labeled "¡Sácame de aquí!" (Get me out of here!) is visible. The background shows a search results page for "Ivie" with various university logos.

Conexión no confiable

Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **uvpapi.uv.es**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intenta conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

Detalles técnicos

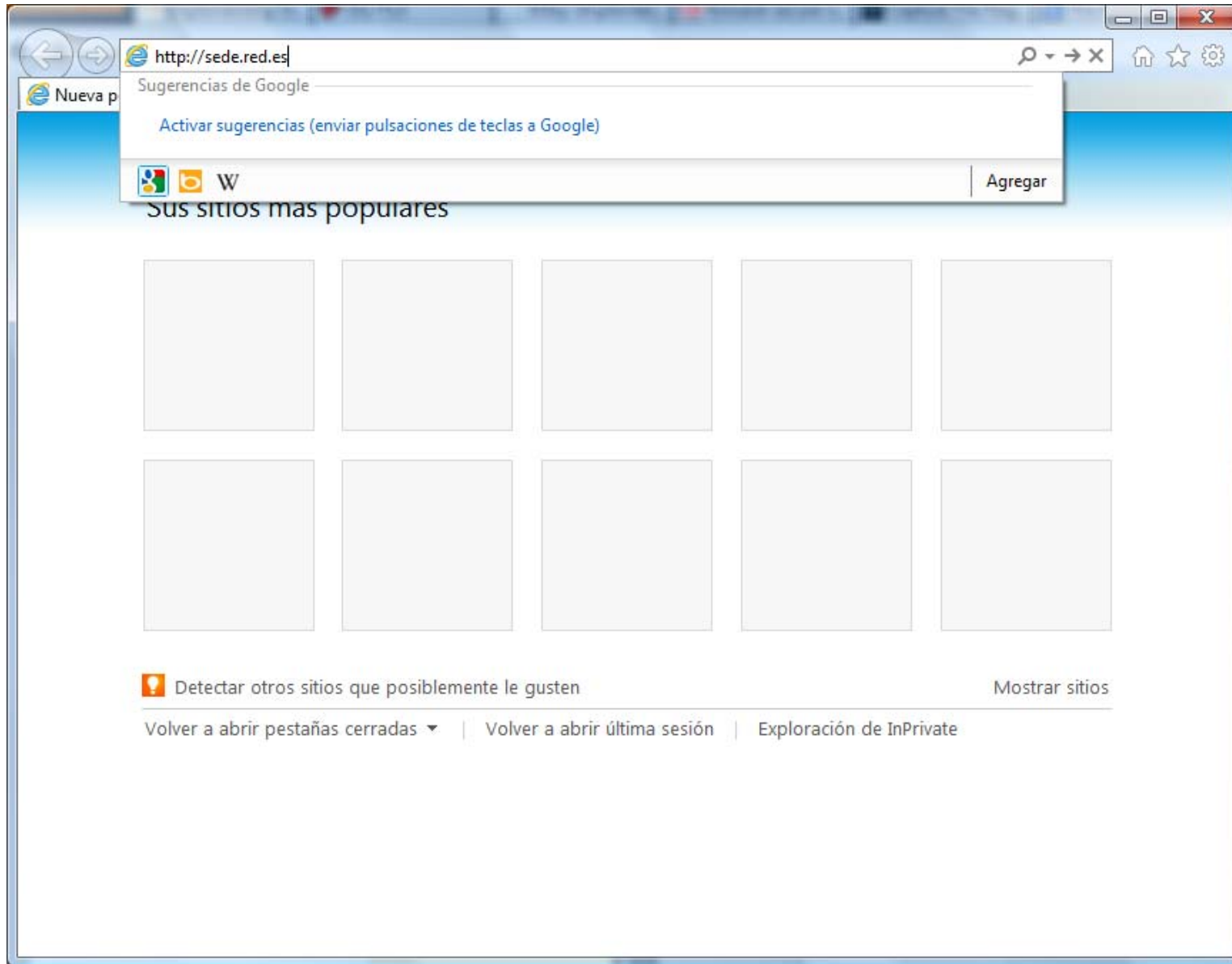
uvpapi.uv.es usa un certificado de seguridad no válido.

No se confía en el certificado porque no se ha proporcionado la cadena de emisor. El certificado sólo es válido para mmedia.uv.es.

(Código de error: sec_error_unknown_issuer)

Entiendo los riesgos

Ejemplo 3: mareando al usuario (1/3)



Ejemplo 3: mareando al usuario (2/3)



The screenshot shows a web browser window displaying the Red.es website. The address bar shows the URL <https://sede.red.gob.es/sede/>. The page header includes the date 24/11/2012 and a security report icon. The main content area features the Red.es logo and navigation icons for red.es, ONTSI, dominios, and RedIRIS. A prominent red banner reads 'Sede Electrónica'. Below this, a section titled 'Trámites en Línea' provides information about online services. A sidebar on the left contains contact information for Red.es support.

24/11/2012

Impulsamos la Sociedad en red

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO red.es

red.es ONTSI .es RedIRIS

Sede Electrónica

Red.es pone a su disposición la dirección de correo electrónico, soporte@sede.red.gob.es, donde pueden presentar sus consultas e informar sobre incidencias, será atendida los días laborables en horario de 9:00 a 19:00h.

Trámites en Línea

La sede electrónica de Red.es facilita el acceso a todos los servicios de Administración Electrónica que red.es pone a disposición de ciudadanos y empresas, en cumplimiento a lo establecido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

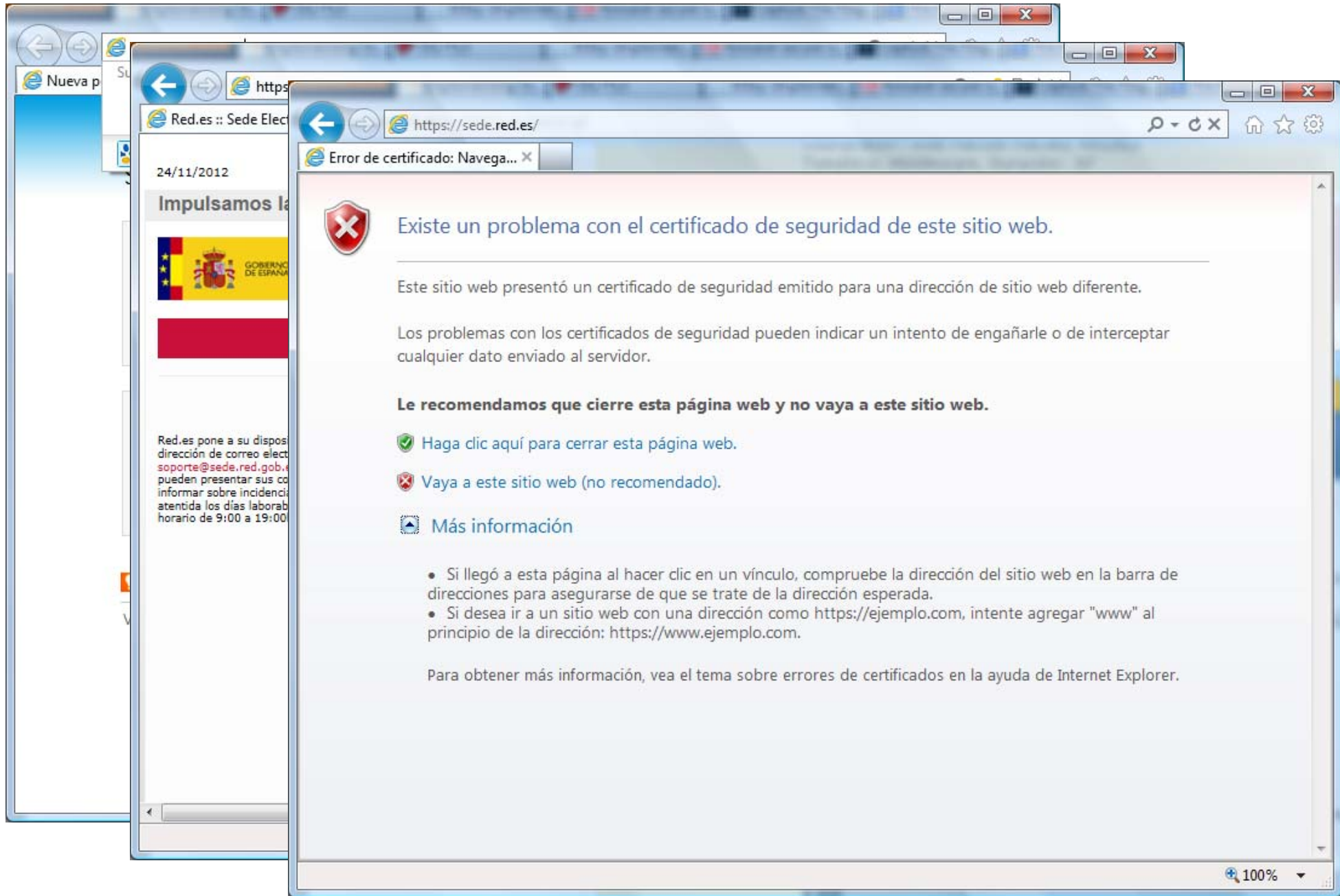
La sede electrónica alberga el Registro Electrónico de Red.es que le permite interactuar telemáticamente con la sede electrónica para la presentación de escritos, solicitudes y comunicaciones relativas a los procedimientos administrativos especificados en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

PROCEDIMIENTOS DISPONIBLES

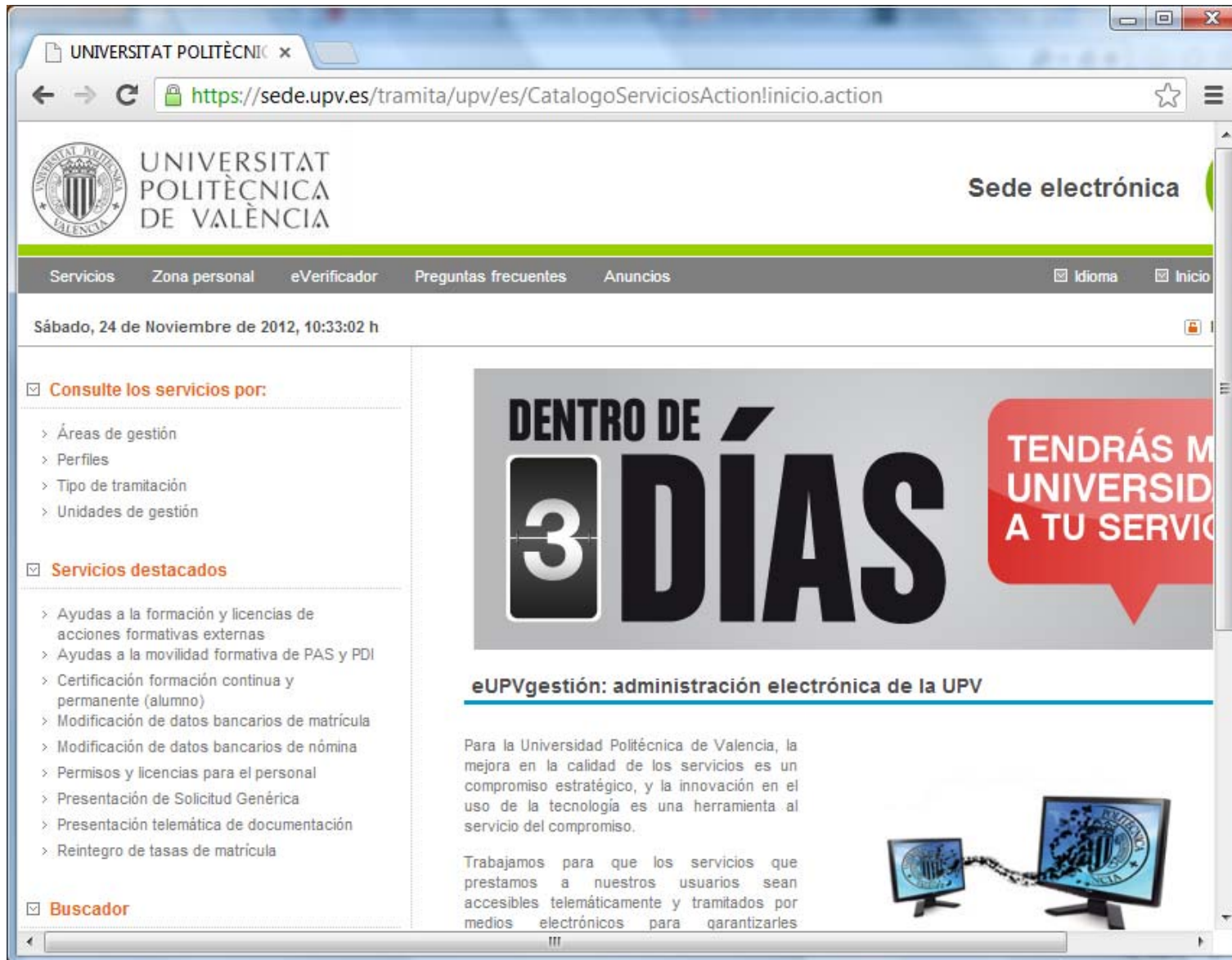
- 1. **Quejas y Sugerencias** (1): Procedimiento telemático para poner en conocimiento de la entidad disfunciones o deficiencias de los servicios. Las quejas no tendrán en ningún caso la calificación de recurso administrativo ni su interposición paralizará el procedimiento establecido en la normativa vigente.
La presentación de una queja no condiciona el ejercicio de las acciones o derechos que, de conformidad con la normativa reguladora de cada procedimiento, puedan ejercitar quienes figuren en él como interesados.
- 2. **Solicitud genérica** (1): Procedimiento telemático que permite presentar cualquier solicitud, escrito o comunicación.

100%

Ejemplo 3: mareando al usuario (3/3)

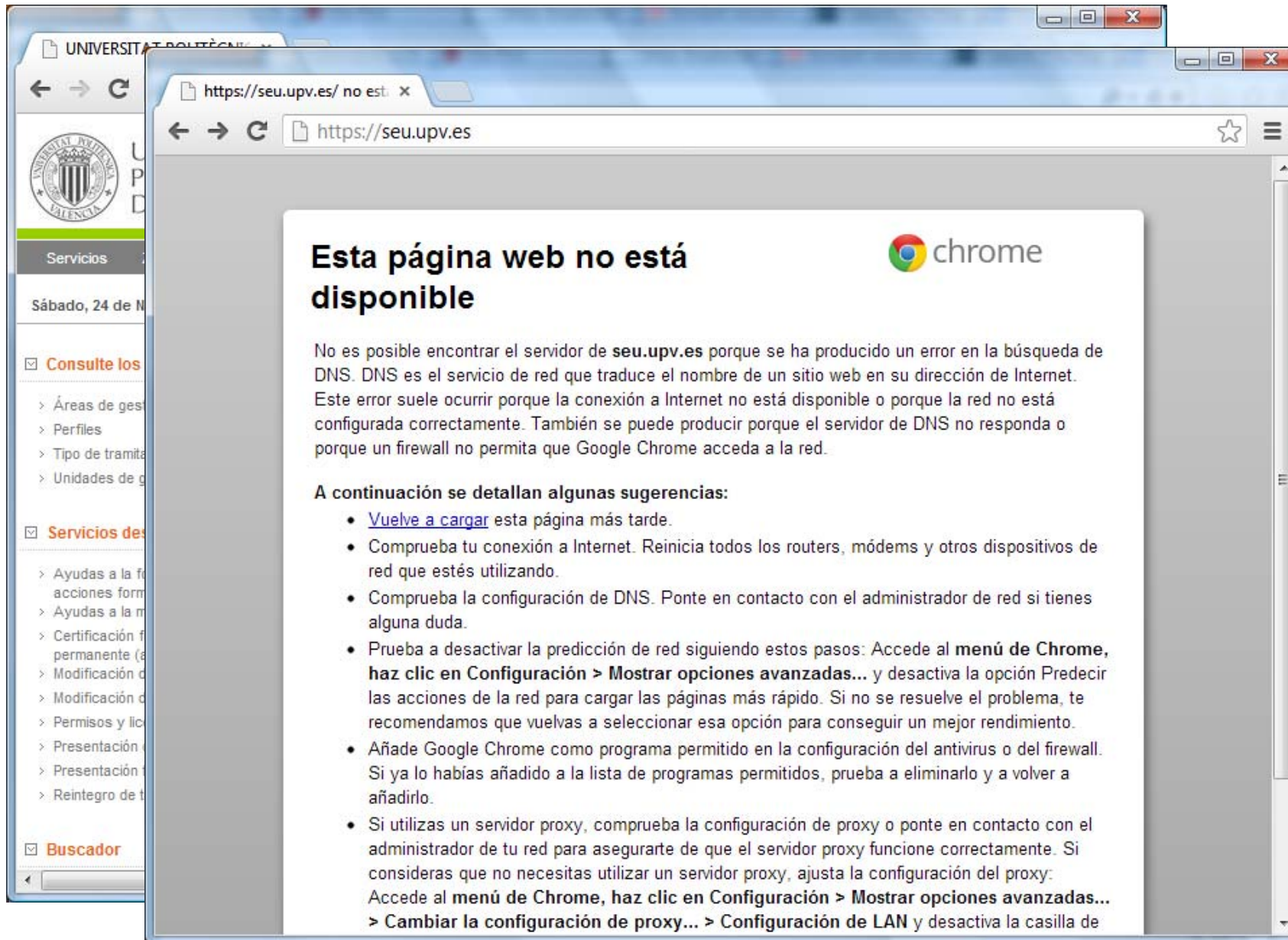


Ejemplo 4: mareando al usuario (1/3)



The screenshot shows a web browser window with the URL <https://sede.upv.es/tramita/upv/es/CatalogoServiciosActionInicio.action>. The page header includes the UPV logo and the text "UNIVERSITAT POLITÈCNICA DE VALÈNCIA" and "Sede electrónica". A navigation menu contains links for "Servicios", "Zona personal", "eVerificador", "Preguntas frecuentes", and "Anuncios", along with "Idioma" and "Inicio" options. The date and time "Sábado, 24 de Noviembre de 2012, 10:33:02 h" are displayed. On the left, there are two sections: "Consulte los servicios por:" with sub-links for "Áreas de gestión", "Perfiles", "Tipo de tramitación", and "Unidades de gestión"; and "Servicios destacados" with a list of services including "Ayudas a la formación y licencias de acciones formativas externas", "Ayudas a la movilidad formativa de PAS y PDI", "Certificación formación continua y permanente (alumno)", "Modificación de datos bancarios de matrícula", "Modificación de datos bancarios de nómina", "Permisos y licencias para el personal", "Presentación de Solicitud Genérica", "Presentación telemática de documentación", and "Reintegro de tasas de matrícula". A "Buscador" field is also present. The main content area features a large banner with the text "DENTRO DE 3 DÍAS" and "TENDRÁS MÁS UNIVERSIDAD A TU SERVICIO". Below the banner, the heading "eUPVgestión: administración electrónica de la UPV" is followed by a paragraph: "Para la Universidad Politécnica de Valencia, la mejora en la calidad de los servicios es un compromiso estratégico, y la innovación en el uso de la tecnología es una herramienta al servicio del compromiso." and another paragraph: "Trabajamos para que los servicios que prestamos a nuestros usuarios sean accesibles telemáticamente y tramitados por medios electrónicos para garantizarles". An image of two computer monitors is shown at the bottom right.

Ejemplo 4: mareando al usuario (2/3)



Ejemplo 4: mareando al usuario (3/3)

The screenshot shows a web browser window displaying the website of the Universitat Politècnica de València. The browser's address bar shows the URL `https://sede.upv.es/tramita/upv/es/CatalogoServiciosActionInicio.action`. A dialog box titled "Certificado" is open, showing the details of a certificate. The dialog box has three tabs: "General", "Detalles", and "Ruta de certificación". The "General" tab is selected, and a table lists the certificate's properties. The table has two columns: "Campo" and "Valor".

Campo	Valor
Puntos de distribución CRL	[1]Punto de distribución CRL: ...
Acceso a la información de ...	[1]Acceso a información de au...
Nombre alternativo del sujeto	Nombre DNS=sede.upv.es, N...
Uso de la clave	Firma digital, Cifrado de clave ...
Restricciones básicas	Tipo de asunto=Entidad final, ...
Algoritmo de identificación	sha1
Huella digital	7f 81 2a 75 e4 ef 6a 37 3c 61 ...

Below the table, the following text is displayed:

```
Nombre DNS=sede.upv.es
Nombre DNS=eupvgestion.upv.es
Nombre DNS=seu.upv.es
```

At the bottom of the dialog box, there are two buttons: "Modificar propiedades..." and "Copiar en archivo...". A link "Más información acerca de los detalles del certificado" is also present. The "Aceptar" button is at the bottom right of the dialog box.

Ejemplo 5: certificado raíz (1/2)

Firefox

060 - Ciudadanos - 060

www.060.es

Google

mapa web | contactar
Benvinguts Benvidos Ongi Etorri Welcome

GOBIERNO DE ESPAÑA

en línea Buscadores temáticos Guía del Estado Participación ciudadana

Buscar...

mi060.es
Usuario/contraseña Certificado

CIUDADANÍA

Salud, seguridad y consumo
Los contenidos agrupados aquí te orientarán en temas médicos y de seguridad, así como en servicios de ayuda al consumidor.

Impuestos, pensiones y ayudas
Aquí podrás iniciar tus gestiones para la declaración de la renta o solicitar ayudas de carácter social.

Documentos personales
Conoce e inicia los trámites relacionados con tu identidad, tales como obtener el DNI, el pasaporte o la tarjeta sanitaria.

Medio ambiente
Aquí encontrarás información sobre energías renovables, biodiversidad y otros temas relacionados con nuestro entorno.

EMPRESAS

Sobre 060

- ¿Qué es la red 060?
- Contacta con nosotros

Se necesita un plugin para mostrar este contenido.
[Instalar plugin...](#)

Novedades 060

- Ley 10/2012, de 20 de noviembre, por la que se regulan determinadas tasas en el ámbito de la Administración de Justicia y del Instituto Nacional de Toxicología y

https://mi060.060.es/060/appmanager/portal/desktop/page/mi060

Ejemplo 5: certificado raíz (2/2)

The image shows a Firefox browser window with a security warning overlay. The warning is titled "Esta conexión no está verificada" (This connection is not verified). It explains that Firefox was asked to connect securely to **mi060.060.es**, but it cannot confirm the connection is secure. It notes that normally, secure connections show verified information, but the identity of this site cannot be verified. A button labeled "¡Sácame de aquí!" (Get me out of here!) is provided. Below, under "Detalles técnicos" (Technical details), it states that **mi060.060.es** uses an invalid security certificate and that the browser does not trust the issuer. The error code is `sec_error_untrusted_issuer`. A section titled "Entiendo los riesgos" (I understand the risks) is also visible.

Firefox - Ciudadanos - 060

www.060.es

en línea Buscadores temáticos Guía del Es

Buscar...

CIUDADANÍA

ión
s ampliar tus estudios, aquí
rás las principales ofertas de
n en España.

y transporte
apartado puedes consultar cuántos
enes en tu carné, pagar una multa o
un viaje.

turismo y ocio
ontrarás una amplia oferta de
es para tu tiempo libre, desde teatro y
ones hasta parques naturales.

a
s mudarte o rehabilitar tu casa, aquí
onsultar datos catastrales,
los de habitabilidad y la normativa

quí podrás inscribirte en la oferta de
úblico de diversos ministerios, así
ormarte sobre tu vida laboral.


https://mi060.060.es/060/appmanager/port

Firefox

Conexión no confiable

https://mi060.060.es/060/appmanager/portal/desktop/page/mi060

Google



Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **mi060.060.es**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

▼ Detalles técnicos

mi060.060.es usa un certificado de seguridad no válido.

No se confía en el certificado porque no se confía en el certificado emisor.

(Código de error: `sec_error_untrusted_issuer`)

▶ Entiendo los riesgos

Ejemplo 6: certificado raíz (1/2)

The image shows a screenshot of a web browser displaying the 'Sede Electrónica' of the Spanish Social Security system. The browser is Firefox, and the address bar shows the URL: https://sede.seg-social.gob.es/Sede_1/ServiciosenLinea/Ciudadanos/166081. The page header includes the Spanish flag, the coat of arms, and the text 'GOBIERNO DE ESPAÑA' and 'MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL'. The main heading is 'Seguridad Social sede Electrónica'. Below this, there are navigation tabs for 'Inicio', 'Ciudadanos', 'Empresas y Profesionales', 'Administraciones y Mutuas', and 'Tablón de Edictos y Anuncios'. A search bar is also present. The main content area is titled 'SERVICIO A CIUDADANOS' and features a prominent link 'Obtener Cita Previa' with a sub-link 'Acceso al servicio'. At the bottom, there are links for 'Mapa de la Sede', 'Accesibilidad', 'Normativa y Legislación', 'Requisitos Técnicos', 'Certificados Digitales', and 'Fecha y Hora Oficial'. The footer contains copyright information: 'Copyright © Seguridad Social. 2012. Todos los derechos reservados. Aviso Legal.' and icons for RSS, W3C AA UCAG, W3C HTML 4.0, and W3C CSS.

Ejemplo 6: certificado raíz (2/2)

The image shows a Firefox browser window displaying a security warning. The browser's address bar shows the URL `https://sede.seg-social.gob.es/Sede_1/Lanzadera/index.htm?URL=104`. The page content includes the logo of the Spanish Government and the Ministry of Employment and Social Security, along with the text 'Seguridad Social sede Electrónica'. A prominent yellow warning box is overlaid on the page, containing the following text:

Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a `w6.seg-social.es`, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intenta conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

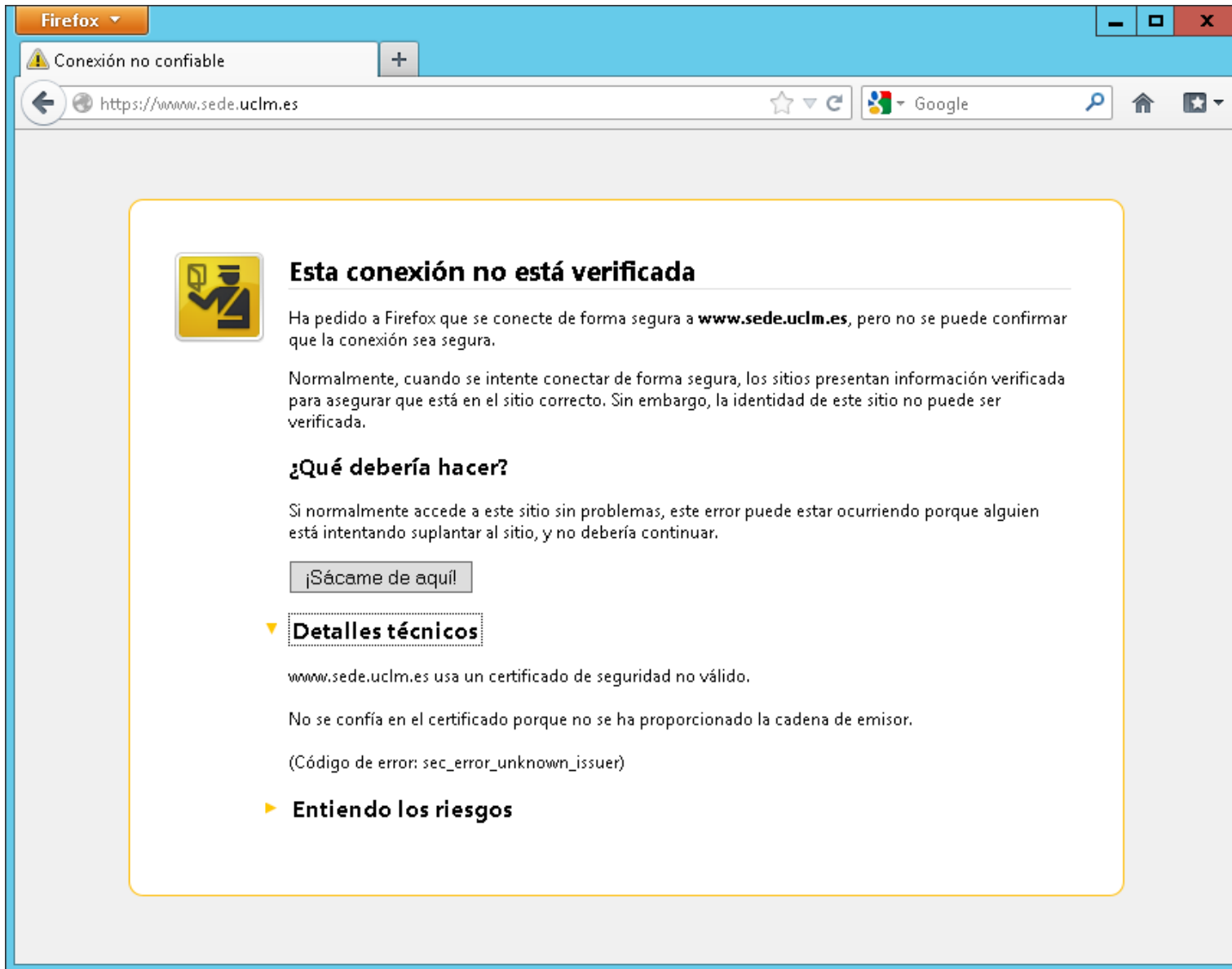
▼ Detalles técnicos

`w6.seg-social.es` usa un certificado de seguridad no válido.

No se confía en el certificado porque no se confía en el certificado emisor.

(Código de error: `sec_error_untrusted_issuer`)

Ejemplo 7: cadena errónea (1/3)



Firefox

Conexión no confiable

https://www.sede.uclm.es

Google

Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **www.sede.uclm.es**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

[¡Sácame de aquí!](#)

▼ Detalles técnicos

www.sede.uclm.es usa un certificado de seguridad no válido.

No se confía en el certificado porque no se ha proporcionado la cadena de emisor.

(Código de error: sec_error_unknown_issuer)

► Entiendo los riesgos

Ejemplo 7: cadena errónea (2/3)

Firefox

Conexión no confiable

Firefox

Conexión no confiable

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Sede electrónica

Servicios Zona personal eVerificador Preguntas frecuentes Anuncios Idioma Inicio

Viernes, 23 de Noviembre de 2012, 20:04:44 h

Consulte los servicios por:

- > Áreas de gestión
- > Perfiles
- > Tipo de tramitación
- > Unidades de gestión

Servicios destacados

- > Ayudas a la formación y licencias de acciones formativas externas
- > Ayudas a la movilidad formativa de PAS y PDI
- > Certificación formación continua y permanente (alumno)
- > Modificación de datos bancarios de matrícula
- > Modificación de datos bancarios de nómina
- > Permisos y licencias para el personal
- > Presentación de Solicitud Genérica
- > Presentación telemática de documentación
- > Reintegro de tasas de matrícula

Buscador

DENTRO DE 4 DÍAS

TENDRÁS MÁS UNIVERSIDAD A TU SERVICIO

eUPVgestión: administración electrónica de la UPV

Para la Universidad Politècnica de Valencia, la mejora en la calidad de los servicios es un compromiso estratégico, y la innovación en el uso de la tecnología es una herramienta al servicio del compromiso.

Trabajamos para que los servicios que prestamos a nuestros usuarios sean accesibles telemáticamente y tramitados por medios electrónicos para garantizarles

Ejemplo 7: cadena errónea (3/3)

The screenshot shows a Firefox browser window with a warning icon in the address bar and the text "Conexión no confiable". The browser's address bar shows the URL "https://www.sede.uclm.es/unitramita/uclm/es/CatalogoServiciosActionInicio.action". The website content includes the UCLM logo and a navigation menu with the following items: "Procedimientos disponibles", "Área personal", "Verificación de documentos", and "Inicio".

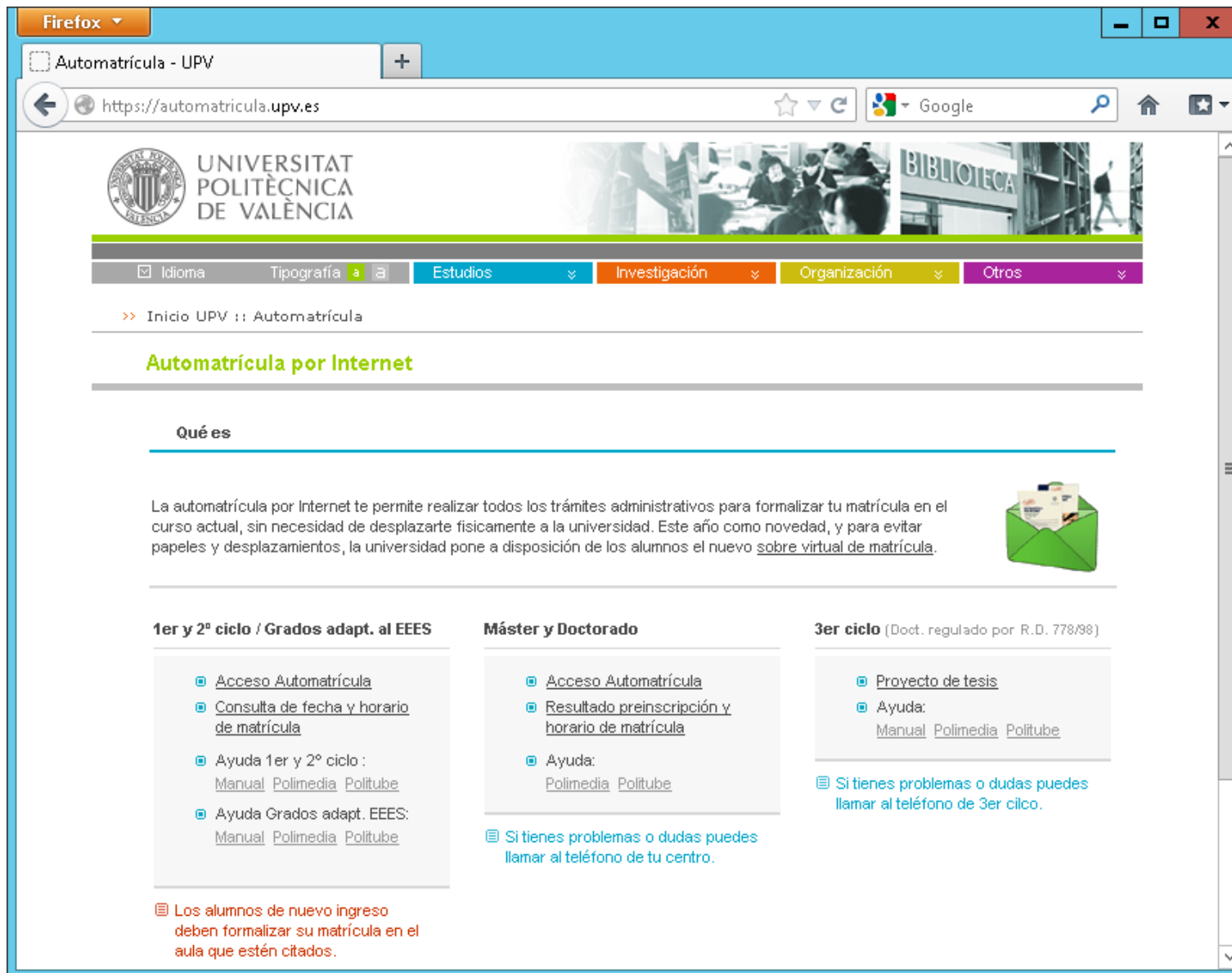
Administración Electrónica en la UCLM: El camino hacia la excelencia

La Universidad de Castilla-La Mancha, como parte de su modelo de Ex la Gestión, tiene el compromiso estratégico de caminar hacia una Ad Universitaria sin papeles, para que la comunidad universitaria profesores, investigadores, personal de administración y servicios, ciudadanos en general, puedan relacionarse con ésta mediar electrónicos. Esta plataforma refleja la realidad de este compromiso través de ella se podrán realizar los procedimientos administrativos e que puedan realizarse por estos medios, tanto en su inicio por el mie comunidad universitaria o el ciudadano, como su tramitación, se conclusión. Todo ello con plena validez y seguridad jurídica. Los ser ofrecidos se han definido conforme al modelo europeo de excele siguiendo las directrices marcadas por la ley 11/2007 de Acceso Ele los Ciudadanos a los Servicios Públicos (LAECSP), el Decreto 12/2010 de Comunidades de Castilla-La Mancha y, finalmente, por la Normative Medios Electrónicos de la propia Universidad de Castilla-La Mancha.

Servicios Ofrecidos

La plataforma ofrece los medios necesarios para aplicar Ad Electrónica a cualquier procedimiento administrativo. En primer lugar s SOLICITUD GENÉRICA, que permite a cualquier ciudadano, sea mie

Ejemplo 8: contenido mixto (1/5)



The screenshot shows a Firefox browser window displaying the website 'Automatrícula - UPV'. The address bar shows 'https://automatricula.upv.es'. The page header features the UPV logo and navigation menus for 'Idioma', 'Tipografía', 'Estudios', 'Investigación', 'Organización', and 'Otros'. The main content area is titled 'Automatrícula por Internet' and includes a section 'Qué es' with a paragraph explaining the online registration process and an icon of a green envelope. Below this, there are three columns of links for different academic levels: '1er y 2º ciclo / Grados adapt. al EEES', 'Máster y Doctorado', and '3er ciclo (Doct. regulado por R.D. 778/98)'. A red notice at the bottom left states that new students must register in person.

Firefox Automatrícula - UPV

https://automatricula.upv.es

UNIVERSITAT POLITÈCNICA DE VALÈNCIA


Idioma Tipografía Estudios Investigación Organización Otros

>> Inicio UPV :: Automatrícula

Automatrícula por Internet

Qué es

La automatrícula por Internet te permite realizar todos los trámites administrativos para formalizar tu matrícula en el curso actual, sin necesidad de desplazarte físicamente a la universidad. Este año como novedad, y para evitar papeles y desplazamientos, la universidad pone a disposición de los alumnos el nuevo [sobre virtual de matrícula](#).



1er y 2º ciclo / Grados adapt. al EEES

- Acceso Automatrícula
- Consulta de fecha y horario de matrícula
- Ayuda 1er y 2º ciclo :
[Manual](#) [Polimedia](#) [Politube](#)
- Ayuda Grados adapt. EEES:
[Manual](#) [Polimedia](#) [Politube](#)

Máster y Doctorado

- Acceso Automatrícula
- Resultado preinscripción y horario de matrícula
- Ayuda:
[Polimedia](#) [Politube](#)
- Si tienes problemas o dudas puedes llamar al teléfono de tu centro.

3er ciclo (Doct. regulado por R.D. 778/98)

- Proyecto de tesis
- Ayuda:
[Manual](#) [Polimedia](#) [Politube](#)
- Si tienes problemas o dudas puedes llamar al teléfono de 3er ciclo.

Los alumnos de nuevo ingreso deben formalizar su matrícula en el aula que estén citados.

Ejemplo 8: contenido mixto (2/5)

Firefox

Automatricula - UPV

UPV


- [Idioma](#)
- Tipografía T
- [Estudios](#) a a m m
- [Investigación](#) a a ñ ñ
- [Organización](#) o o
- [Otros](#)

[Inicio UPV](#) :: [Automatricula](#)

Automatricula por Internet

Qué es

La automatricula por Internet te permite realizar todos los trámites administrativos para formalizar tu matrícula en el curso actual, sin necesidad de desplazarte físicamente a la universidad. Este año como novedad, y para evitar papeles y desplazamientos, la universidad pone a disposición de los alumnos el nuevo [sobre virtual de matrícula](#).



1er y 2º ciclo / Grados **Máster y Doctorado** **3er ciclo (Doct. regulado por adapt. al E...**

Solo se visualiza el contenido seguro. [¿Qué riesgo existe?](#) [Mostrar todo el contenido](#)

100%

Ejemplo 8: contenido mixto (3/5)

The screenshot shows a Firefox browser window displaying the website <https://automatricula.upv.es/>. The page header features the logo of the Universitat Politècnica de València and a navigation menu with categories: Idioma, Tipografía, Estudios, Investigación, Organización, and Otros. The main content area is titled "Automatrícula por Internet" and includes a section "Qué es" with a description of the online registration process and an icon of a green envelope. Below this, there are three columns of links for different academic levels: "1er y 2º ciclo / Grados adapt. al EEES", "Máster y Doctorado", and "3er ciclo (Doct. regulado por R.D. 778/98)". A red notice at the bottom states: "Los alumnos de nuevo ingreso deben formalizar su matrícula en el aula que estén citados."

Firefox

Automatrícula - UPV

https://automatricula.upv.es/

UNIVERSITAT POLITÈCNICA DE VALÈNCIA


Idioma Tipografía Estudios Investigación Organización Otros

>> Inicio UPV :: Automatrícula

Automatrícula por Internet

Qué es

La automatría por Internet te permite realizar todos los trámites administrativos para formalizar tu matrícula en el curso actual, sin necesidad de desplazarte físicamente a la universidad. Este año como novedad, y para evitar papeles y desplazamientos, la universidad pone a disposición de los alumnos el nuevo sobre virtual de matrícula.



1er y 2º ciclo / Grados adapt. al EEES

- Acceso Automatrícula
- Consulta de fecha y horario de matrícula
- Ayuda 1er y 2º ciclo :
[Manual](#) [Polimedia](#) [Politube](#)
- Ayuda Grados adapt. EEES:
[Manual](#) [Polimedia](#) [Politube](#)

Los alumnos de nuevo ingreso deben formalizar su matrícula en el aula que estén citados.

Máster y Doctorado

- Acceso Automatrícula
- Resultado preinscripción y horario de matrícula
- Ayuda:
[Polimedia](#) [Politube](#)

Si tienes problemas o dudas puedes llamar al teléfono de tu centro.

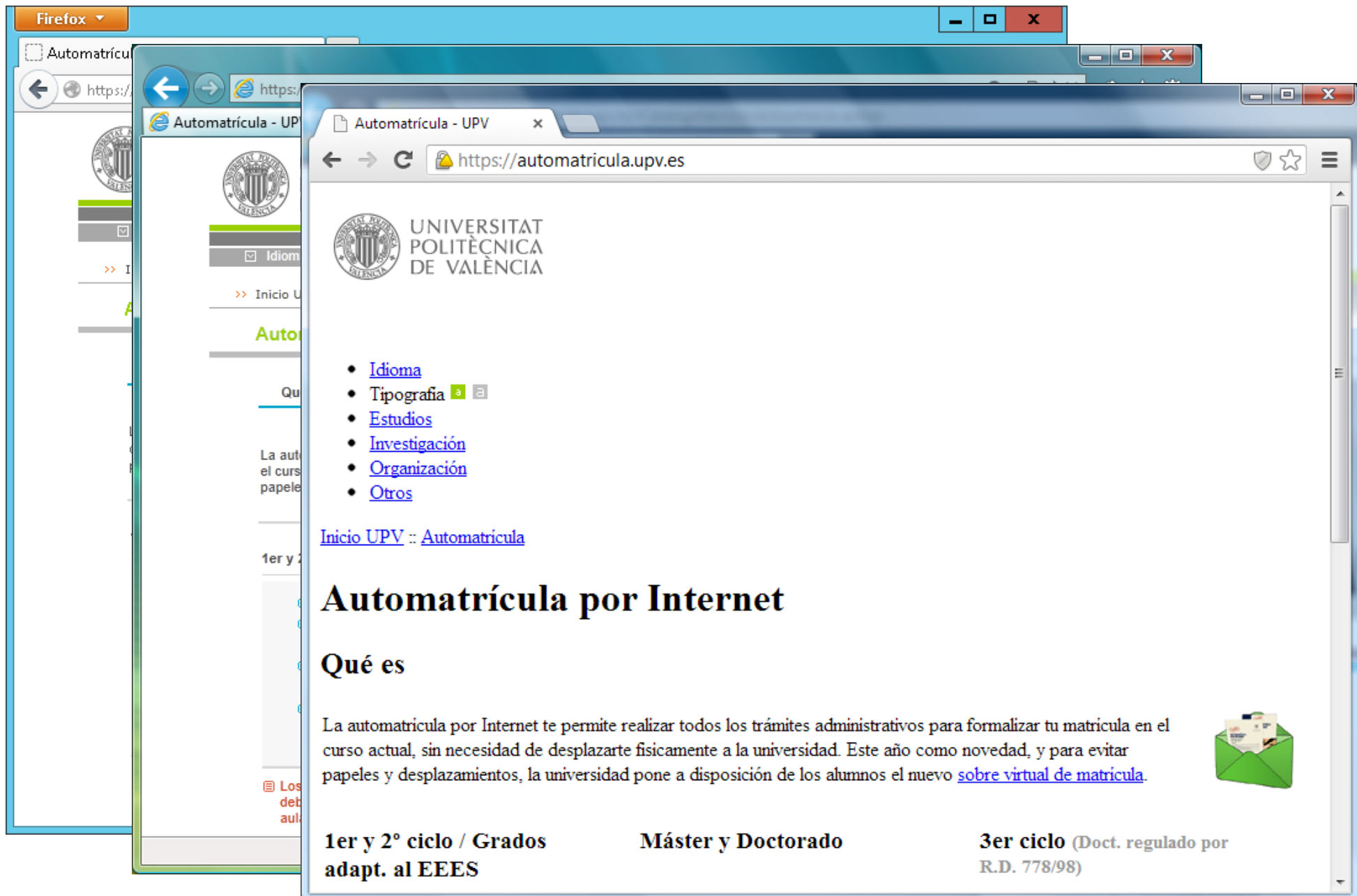
3er ciclo (Doct. regulado por R.D. 778/98)

- Proyecto de tesis
- Ayuda:
[Manual](#) [Polimedia](#) [Politube](#)

Si tienes problemas o dudas puedes llamar al teléfono de 3er ciclo.

100%

Ejemplo 8: contenido mixto (4/5)




Firefox

Automatricula - UPV

https://automatricula.upv.es

UNIVERSITAT POLITÈCNICA DE VALÈNCIA


- [Idioma](#)
- Tipografia 
- [Estudios](#)
- [Investigación](#)
- [Organización](#)
- [Otros](#)

[Inicio UPV](#) :: [Automatricula](#)

Automatricula por Internet

Qué es

La automatricula por Internet te permite realizar todos los trámites administrativos para formalizar tu matricula en el curso actual, sin necesidad de desplazarte físicamente a la universidad. Este año como novedad, y para evitar papeles y desplazamientos, la universidad pone a disposición de los alumnos el nuevo [sobre virtual de matricula](#).



1er y 2º ciclo / Grados adapt. al EEES **Máster y Doctorado** **3er ciclo (Doct. regulado por R.D. 778/98)**

Ejemplo 8: contenido mixto (5/5)

Firefox

Automatricula - UPV

https://automatricula.upv.es

UNIVERSITAT POLITÈCNICA DE VALÈNCIA


Idioma Tipografía Estudios Investigación Organización Otros

>> Inicio UPV :: Automatricula

Automatricula por Internet

Qué es

La automatricula por Internet te permite realizar todos los trámites administrativos para formalizar tu matrícula en el curso actual, sin necesidad de desplazarte físicamente a la universidad. Este año como novedad, y para evitar papeles y desplazamientos, la universidad pone a disposición de los alumnos el nuevo [sobre virtual de matrícula](#).



1er y 2º ciclo / Grados adapt. al EEES	Máster y Doctorado	3er ciclo (Doct. regulado por R.D. 778/98)
<ul style="list-style-type: none">Acceso AutomatriculaConsulta de fecha y horario de matrículaAyuda 1er y 2º ciclo : Manual Polimedia PolitubeAyuda Grados adapt. EEES: Manual Polimedia Politube	<ul style="list-style-type: none">Acceso AutomatriculaResultado preinscripción y horario de matrículaAyuda: Polimedia Politube <p>Si tienes problemas o dudas puedes llamar al teléfono de tu centro.</p>	<ul style="list-style-type: none">Proyecto de tesisAyuda: Manual Polimedia Politube <p>Si tienes problemas o dudas puedes llamar al teléfono de 3er ciclo.</p>

Los alumnos de nuevo ingreso deben formalizar su matrícula en el aula que estén citados.

Ejemplo 9: otros problemas (1/2)



Firefox

Sede Electrónica de la Universidad Rey J...

https://sede.urjc.es/primera-visita.php

Google

U Universidad Rey Juan Carlos | Sede Electrónica

FECHA Y HORA OFICIAL DE LA SEDE: 24/11/2012 - 12:24:27

SEDE ELECTRÓNICA DE LA UNIVERSIDAD REY JUAN CARLOS / SOPORTE AL USUARIO / PRIMERA VISITA

PRIMERA VISITA A LA SEDE

- > Para el correcto acceso a la Sede Electrónica de la URJC
- ▣ Manual de Usuario de la Sede Electrónica
 - PDF | [Manual de Usuario de la Sede Electrónica de la Universidad Rey Juan Carlos](#)
- ▣ Instale en su navegador los siguientes certificados de seguridad de la Fábrica Nacional de Moneda y Timbre*:
 - 1.-  "Certificado raíz de la AC-Raíz FNMT-RCM". Se puede obtener en: <http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt>
 - 2.-  "Certificado raíz de la AC-APE". Se puede obtener en: <http://www.cert.fnmt.es/certs/ACRAIZAPE.crt>
 - 3.-  "Certificado raíz de la AC-AP". Se puede obtener en: <http://www.cert.fnmt.es/certs/ACADMINISTRACIONPUBLICA.crt>

* Los certificados 1, 2 y 3 también se pueden descargar desde <http://www.cert.fnmt.es>, luego deberemos ir al menú "ADM. PÚBLICA", después a "APE" y finalmente iremos al menú "Certificado Raíz". En dicha página encontramos los 3 Certificados: "Certificado Raíz de la

Navigation icons: Document, Folder, Home, Bookmarks, Clock, Calendar (27)

Ejemplo 9: otros problemas (2/2)

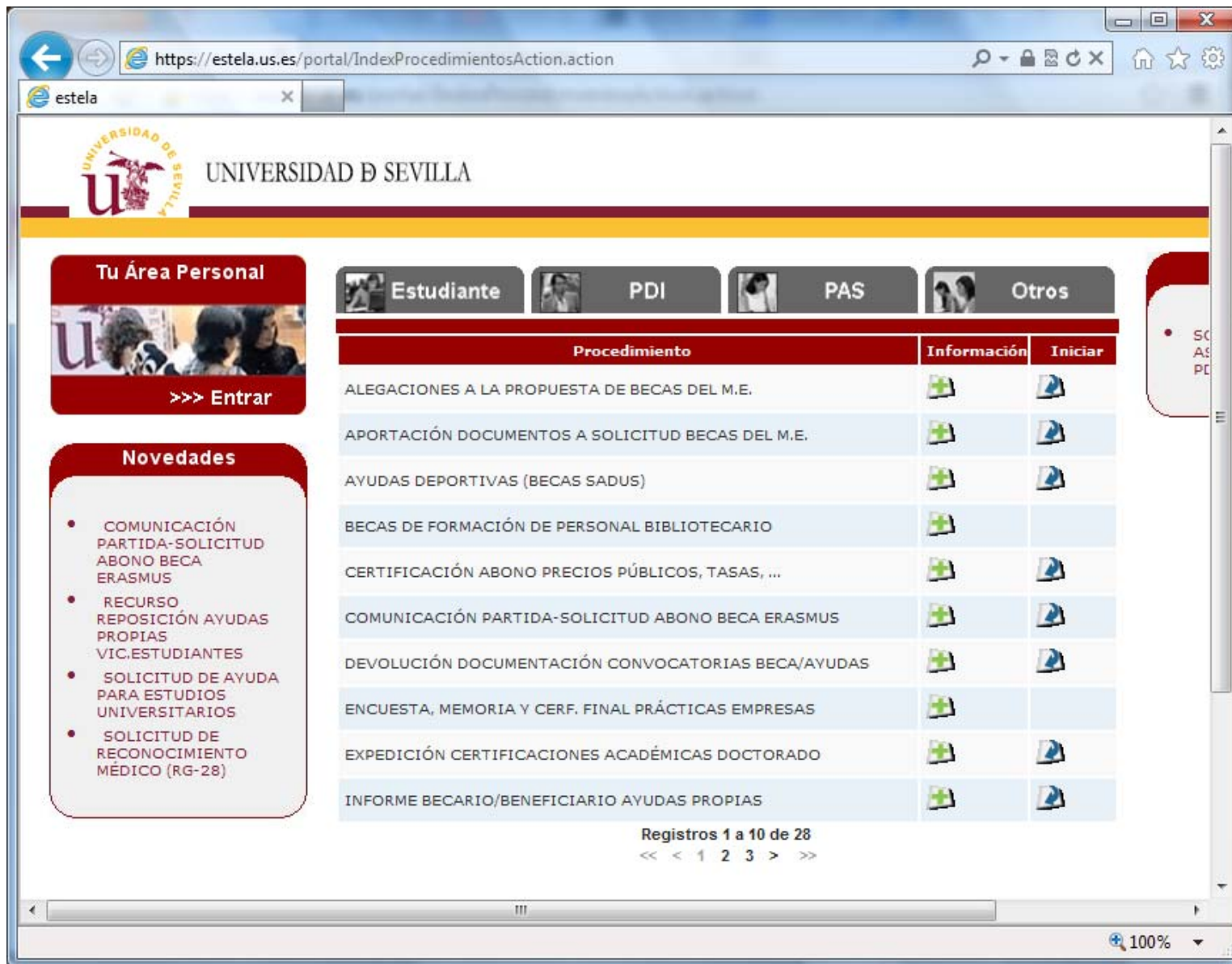
The image shows two overlapping browser windows. The top window displays the website 'Sede Electrónica de la Universidad Rey Juan Carlos'. The bottom window shows the 'Qualys SSL Labs' audit results for the website. The audit report includes the following table:

Protocol	Supported
TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3.0	Yes
SSL 2.0 INSECURE	Yes

Below the table, the 'Cipher Suites (sorted by strength; server has no preference)' section lists several weak ciphers:

- SSL_RC4_128_EXPORT40_WITH_MD5 (0x20080) **WEAK** 40
- SSL_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) **WEAK** 40
- TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK** 40
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK** 40
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **WEAK** 40

Ejemplo 10: otros problemas (1/2)



The screenshot shows a web browser window displaying the portal for the University of Seville. The URL is <https://estela.us.es/portal/IndexProcedimientosAction.action>. The page features the university's logo and name at the top. Below this, there are navigation tabs for 'Estudiante', 'PDI', 'PAS', and 'Otros'. A table lists various procedures with columns for 'Procedimiento', 'Información', and 'Iniciar'. On the left, there are sections for 'Tu Área Personal' and 'Novedades'.

Tu Área Personal

>>> Entrar

Novedades

- COMUNICACIÓN PARTIDA-SOLICITUD ABONO BECA ERASMUS
- RECURSO REPOSICIÓN AYUDAS PROPIAS VIC.ESTUDIANTES
- SOLICITUD DE AYUDA PARA ESTUDIOS UNIVERSITARIOS
- SOLICITUD DE RECONOCIMIENTO MÉDICO (RG-28)

Estudiante **PDI** **PAS** **Otros**

Procedimiento	Información	Iniciar
ALEGACIONES A LA PROPUESTA DE BECAS DEL M.E.		
APORTACIÓN DOCUMENTOS A SOLICITUD BECAS DEL M.E.		
AYUDAS DEPORTIVAS (BECAS SADUS)		
BECAS DE FORMACIÓN DE PERSONAL BIBLIOTECARIO		
CERTIFICACIÓN ABONO PRECIOS PÚBLICOS, TASAS, ...		
COMUNICACIÓN PARTIDA-SOLICITUD ABONO BECA ERASMUS		
DEVOLUCIÓN DOCUMENTACIÓN CONVOCATORIAS BECA/AYUDAS		
ENCUESTA, MEMORIA Y CERF. FINAL PRÁCTICAS EMPRESAS		
EXPEDICIÓN CERTIFICACIONES ACADÉMICAS DOCTORADO		
INFORME BECARIO/BENEFICIARIO AYUDAS PROPIAS		

Registros 1 a 10 de 28
<< < 1 2 3 > >>

100%

Ejemplo 10: otros problemas (2/2)

https://estela.us.es/portal/IndexProcedimientosAction.action

estela

UNIVERSIDAD DE SEVILLA

Tu Área Personal

>>> Entrar

Novedades

- COMUNICACIÓN PARTIDA-SOLICITUD ABONO BECA ERASMUS
- RECURSO REPOSICIÓN AYUDAS PROPIAS VIC. ESTUDIANTES
- SOLICITUD DE AYUDA PARA ESTUDIOS UNIVERSITARIOS
- SOLICITUD DE RECONOCIMIENTO MÉDICO (RG-28)

estela.us.es

Identidad no verificada

Permisos Conexión

La identidad de este sitio web ha sido verificada por FNMT.

No se ha podido comprobar si se ha revocado el certificado.
[Datos del certificado](#)

Tu conexión a estela.us.es está cifrada con codificación de 256 bits.

La conexión utiliza TLS 1.0.

La conexión se ha encriptado mediante AES_256_CBC, con SHA1 para la autenticación del mensaje y con DHE_RSA como mecanismo de intercambio de claves.

La conexión no utiliza la compresión SSL.

El servidor no admite la modificación de renegociación de seguridad de la capa de transporte.

Información del sitio
No has visitado nunca este sitio.

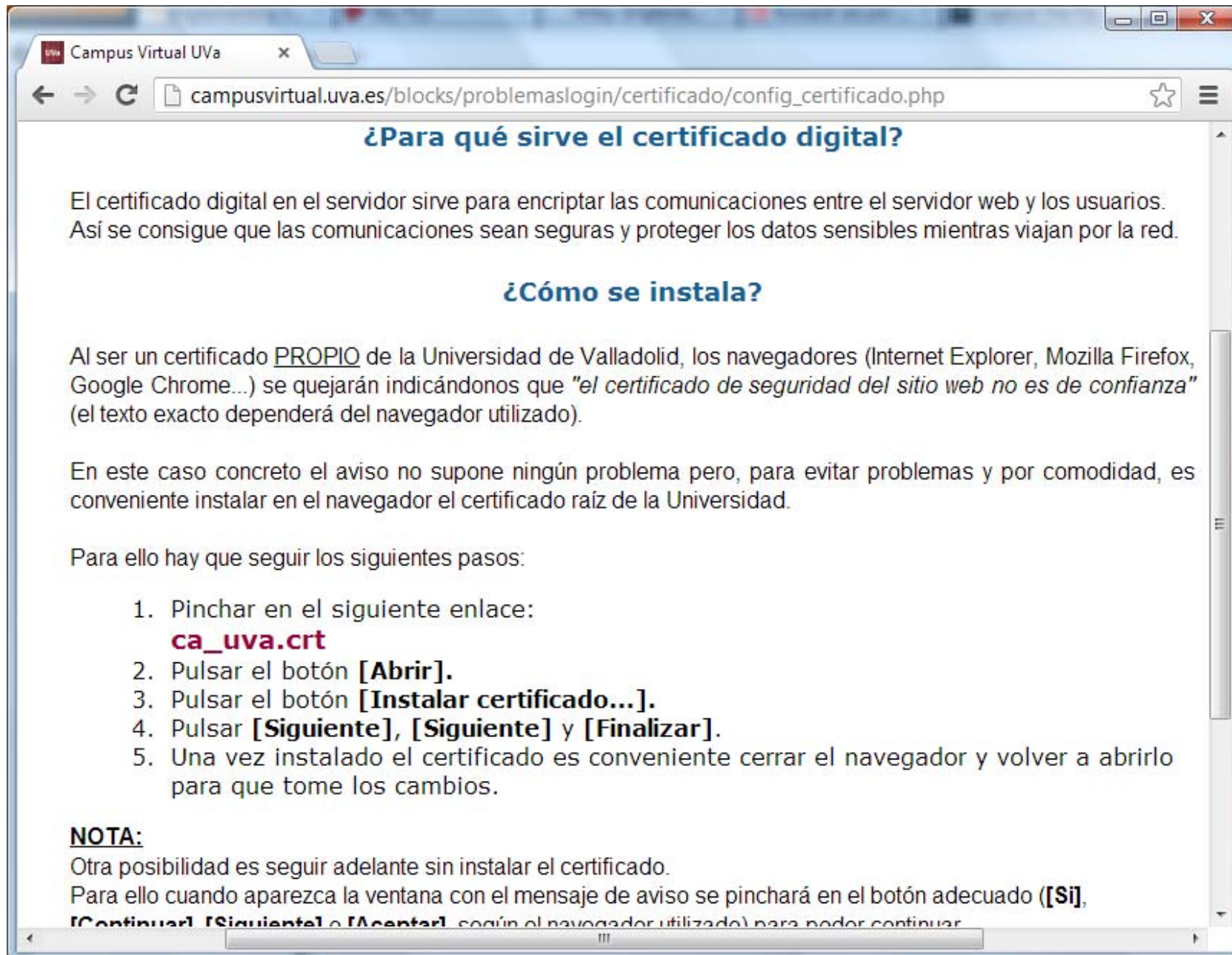
¿Necesitas ayuda?

Procedimiento	Información	Iniciar
LISTA DE BECAS DEL M.E.	+	▶
SOLICITUD BECAS DEL M.E.	+	▶
ERASMUS)	+	▶
PERSONAL BIBLIOTECARIO	+	▶
AYUDAS PÚBLICAS, TASAS, ...	+	▶
SOLICITUD ABONO BECA ERASMUS	+	▶
CONVOCATORIAS BECA/AYUDAS	+	▶
FINAL PRÁCTICAS EMPRESAS	+	▶
AYUDAS ACADÉMICAS DOCTORADO	+	▶
AYUDAS PROPIAS	+	▶

Registros 1 a 10 de 28

<< < 1 2 3 > >>

Ejemplo 11: instrucciones de uso



Campus Virtual UVA

campusvirtual.uva.es/blocks/problemaslogin/certificado/config_certificado.php

¿Para qué sirve el certificado digital?

El certificado digital en el servidor sirve para encriptar las comunicaciones entre el servidor web y los usuarios. Así se consigue que las comunicaciones sean seguras y proteger los datos sensibles mientras viajan por la red.

¿Cómo se instala?

Al ser un certificado PROPIO de la Universidad de Valladolid, los navegadores (Internet Explorer, Mozilla Firefox, Google Chrome...) se quejarán indicándonos que *"el certificado de seguridad del sitio web no es de confianza"* (el texto exacto dependerá del navegador utilizado).

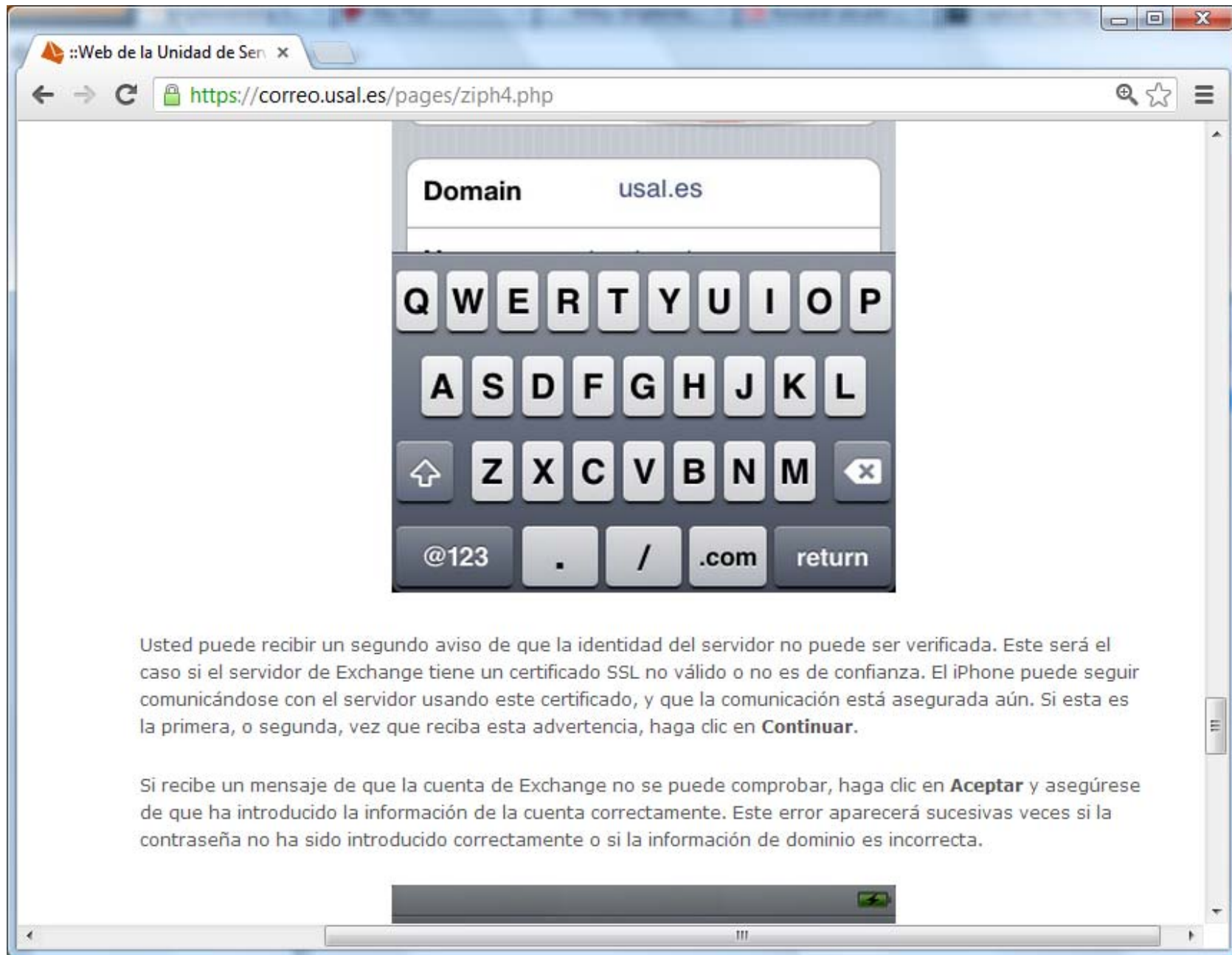
En este caso concreto el aviso no supone ningún problema pero, para evitar problemas y por comodidad, es conveniente instalar en el navegador el certificado raíz de la Universidad.

Para ello hay que seguir los siguientes pasos:

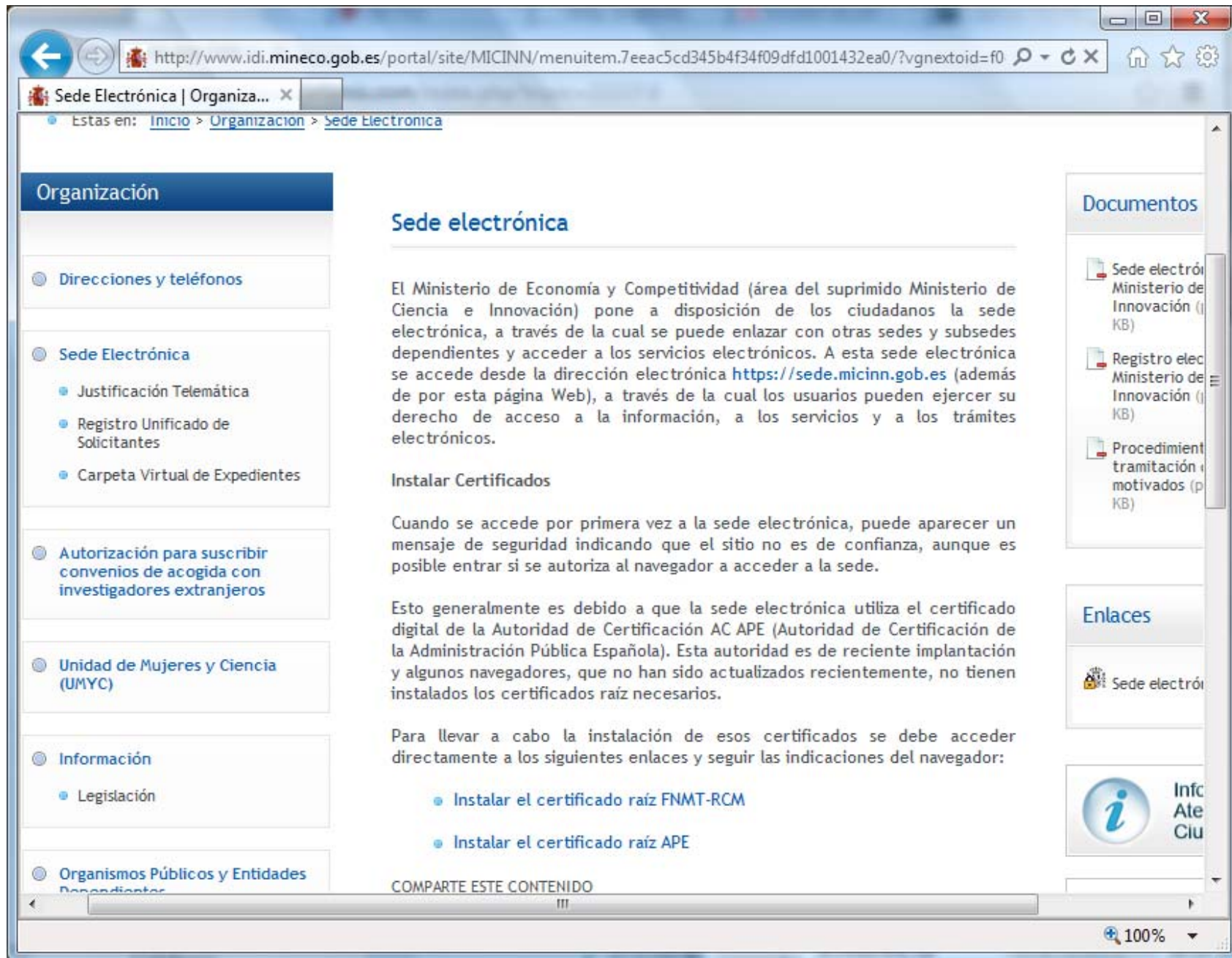
1. Pinchar en el siguiente enlace:
ca_uva.crt
2. Pulsar el botón **[Abrir]**.
3. Pulsar el botón **[Instalar certificado...]**.
4. Pulsar **[Siguiente]**, **[Siguiente]** y **[Finalizar]**.
5. Una vez instalado el certificado es conveniente cerrar el navegador y volver a abrirlo para que tome los cambios.

NOTA:
Otra posibilidad es seguir adelante sin instalar el certificado.
Para ello cuando aparezca la ventana con el mensaje de aviso se pinchará en el botón adecuado (**[Si]**, **[Continuar]**, **[Siguiente]** o **[Aceptar]**, según el navegador utilizado) para poder continuar.

Ejemplo 12: instrucciones de uso



Ejemplo 13: instrucciones de uso



http://www.idi.mineco.gob.es/portal/site/MICINN/menuitem.7eeac5cd345b4f34f09dfd1001432ea0/?vgnnextoid=f0

Estas en: Inicio > Organización > Sede Electrónica

Organización

- Direcciones y teléfonos
- Sede Electrónica**
 - Justificación Telemática
 - Registro Unificado de Solicitantes
 - Carpeta Virtual de Expedientes
- Autorización para suscribir convenios de acogida con investigadores extranjeros
- Unidad de Mujeres y Ciencia (UMYC)
- Información
 - Legislación
- Organismos Públicos y Entidades Dependientes

Sede electrónica

El Ministerio de Economía y Competitividad (área del suprimido Ministerio de Ciencia e Innovación) pone a disposición de los ciudadanos la sede electrónica, a través de la cual se puede enlazar con otras sedes y subsedes dependientes y acceder a los servicios electrónicos. A esta sede electrónica se accede desde la dirección electrónica <https://sede.micinn.gob.es> (además de por esta página Web), a través de la cual los usuarios pueden ejercer su derecho de acceso a la información, a los servicios y a los trámites electrónicos.

Instalar Certificados

Cuando se accede por primera vez a la sede electrónica, puede aparecer un mensaje de seguridad indicando que el sitio no es de confianza, aunque es posible entrar si se autoriza al navegador a acceder a la sede.

Esto generalmente es debido a que la sede electrónica utiliza el certificado digital de la Autoridad de Certificación AC APE (Autoridad de Certificación de la Administración Pública Española). Esta autoridad es de reciente implantación y algunos navegadores, que no han sido actualizados recientemente, no tienen instalados los certificados raíz necesarios.

Para llevar a cabo la instalación de esos certificados se debe acceder directamente a los siguientes enlaces y seguir las indicaciones del navegador:

- Instalar el certificado raíz FNMT-RCM
- Instalar el certificado raíz APE

COMPARTE ESTE CONTENIDO

Documentos

- Sede electrón Ministerio de Innovación (1 KB)
- Registro elec Ministerio de Innovación (1 KB)
- Procedimient tramitación i motivados (p KB)

Enlaces

- Sede electrón

Info Ate Ciu

100%

Algunas consecuencias (1/3)

Firefox

Foros — Portal Guadalinux

www.guadalinux.org/participa/foros/hilo/21319/

CONSEJERÍA DE ECONOMÍA, INNOVACIÓN Y CIENCIA
JUNTA DE ANDALUCÍA

guadalinux.
SOFTWARE LIBRE

Formación Guadalinux
Apúntate a los cursos de Guadalinux..

Ab!

Nombre de Usuario Contraseña Entrar Darse de Alta

Usted está aquí: Inicio → ¡Participa! → Foros

Buscador Buscar

Menú

Portada

- ¿Qué es Guadalinux?
- ¿Dónde estamos?
- Más programas
- Ayuda y soporte
- Foros
- ¡Participa!
- Foros
- Chat
- Encuestas
- Guadalinux por el mundo
- Eventos relacionados

Conexión no confiable.

▲ Volver al foro (Usando **Guadalinux** v7)

Orden: Escalonando las respuestas Cambiar orden

Escrito por miancatri el 30/08/2011 13:34

miancatri  Hola. ¿Qué pasa con las páginas de los organismos públicos que el navegador te dice que no son confiables?. Por ejemplo:
<https://ws003.juntadeandalucia.es/>

Firefox

Adepto Senior
Envíos: 358

Esta conexión no está verificada.

Ha pedido a Firefox que se verifique la conexión a **ws003.juntadeandalucia.es**, pero no se puede verificar. Normalmente, cuando se intenta conectar de un sitio no puede ser verificada.

Re: Conexión no confiable.

Escrito por Chrysaor el 30/08/2011 16:52

Chrysaor 

Pues no pasa nada, simplemente que tu navegador no reconoce esos certificados porque no lo tiene en los certificados verificados. Si estas seguro que esas páginas son las que tienes que entrar (cita médico, correo ciudadano, etc.) verificas el certificado y entras.

1. Pulsas en entiendo los riesgos.
2. Pulsas en añadir excepción
3. Confirmas excepción de seguridad.

Adepto Ancestral
Envíos: 916

Algunas consecuencias (2/3)



The screenshot shows a web browser window with the address bar displaying `www.elforodeltenis.com/index.php?topic=22227.0`. The page content is a forum thread with three replies. Each reply includes the user's name, profile information, a timestamp, the reply text, and an 'En línea' status indicator.

federerfanforever
Colaborador en juego (TCG)
Karma: 28485
 Desconectado
Mensajes: 37.201

Re:"Advertencia: algo falla aquí."
« Respuesta #1 en: 11 de Junio de 2011, 18:59:12 pm »

Bueno, a mí también me sale algo de problemas con el certificado de seguridad de la página web cuando intento entrar a hotmail.com y me recomiendan que no vaya, pero voy y nunca pasa nada, no creo que tenga mayor importancia este asunto 🤔

En línea

cristisis
Karma: 12466
 Desconectado
Mensajes: 10.985

Re:"Advertencia: algo falla aquí."
« Respuesta #2 en: 11 de Junio de 2011, 19:06:41 pm »

Ya es la segunda vez que me ocurre y tengo que darle a "continuar de todos modos" para poder acceder al foro.

En línea

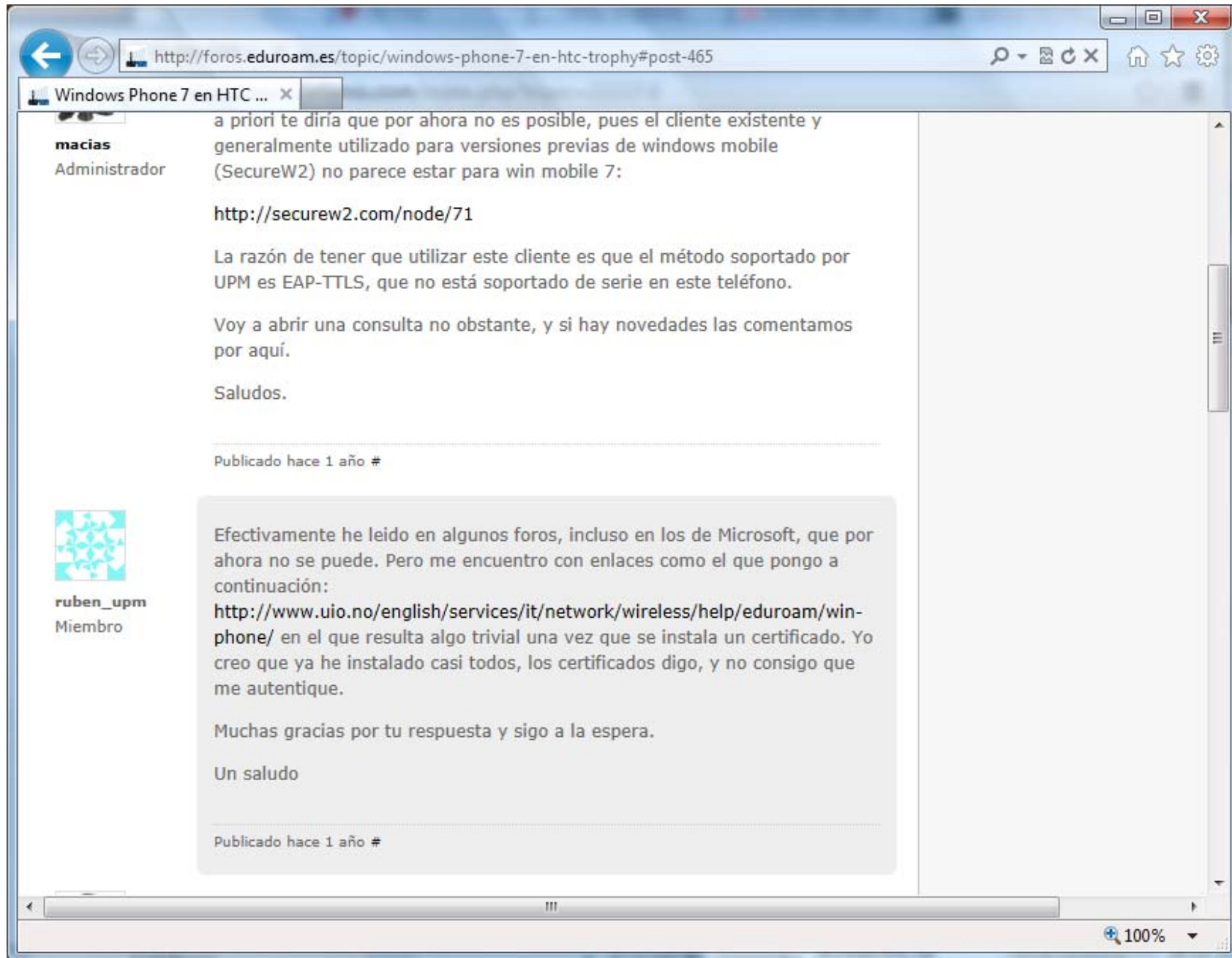
federerfanforever
Colaborador en juego (TCG)
Karma: 28485
 Desconectado
Mensajes: 37.201

Re:"Advertencia: algo falla aquí."
« Respuesta #3 en: 11 de Junio de 2011, 19:17:36 pm »

A mí no me ha pasado nunca al entrar al foro, pero como te digo, me pasa algo parecido con esa otra página y luego es todo agua de borrajas 🤔

En línea

Algunas consecuencias (3/3)



The screenshot shows a web browser window displaying a forum thread. The address bar shows the URL: <http://foros.eduroam.es/topic/windows-phone-7-en-htc-trophy#post-465>. The thread title is "Windows Phone 7 en HTC ...".

The first post is by user **macias** (Administrador). The text of the post is:

a priori te diría que por ahora no es posible, pues el cliente existente y generalmente utilizado para versiones previas de windows mobile (SecureW2) no parece estar para win mobile 7:

<http://securew2.com/node/71>

La razón de tener que utilizar este cliente es que el método soportado por UPM es EAP-TTLS, que no está soportado de serie en este teléfono.

Voy a abrir una consulta no obstante, y si hay novedades las comentamos por aquí.

Saludos.

Publicado hace 1 año #

The second post is by user **ruben_upm** (Miembro). The text of the post is:

Efectivamente he leído en algunos foros, incluso en los de Microsoft, que por ahora no se puede. Pero me encuentro con enlaces como el que pongo a continuación:

<http://www.uio.no/english/services/it/network/wireless/help/eduroam/win-phone/> en el que resulta algo trivial una vez que se instala un certificado. Yo creo que ya he instalado casi todos, los certificados digo, y no consigo que me autentique.

Muchas gracias por tu respuesta y sigo a la espera.

Un saludo

Publicado hace 1 año #

La situación ideal

- El uso de SSL/TLS debería garantizar, en nuestras conexiones:
 - la **confidencialidad**
 - la **integridad**
 - la **autenticidad**
 - la **disponibilidad**
- SSL tiene su origen en la navegación web (nace como una extensión de HTTP), pero hoy en día soporta cualquier tipo de aplicación
 - SMTP, POP, IMAP, FTP, NNTP, etc.
- Tampoco hay que olvidar las conexiones entre servidores (sin interacción de usuario)

SSL / TLS

■ ¿Qué protocolo(s) deberíamos implementar?

✗ SSLv2 (1995): Secure Sockets Layer

- <http://www.mozilla.org/projects/security/pki/nss/ssl/draft02.html>
- Propuesta original de Netscape. Hoy en día es **inseguro**

✓ SSLv3 (1996)

- <http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt>
- Actualmente en uso. Aceptado como base por el IETF

✓ TLS 1.0 (1999): Transport Layer Security

- <http://www.ietf.org/rfc/rfc2246.txt>
- Prácticamente similar a SSLv3. El más utilizado hoy en día

✓ TLS 1.1 (2006): RFC 4346

- Mejora la versión anterior y tiene un gran base de clientes

✓ TLS 1.2 (2008): RFC 5246

- Versión actual (teóricamente). Soportado por IE en W7+

Confidencialidad

- Garantizar la confidencialidad es sencillo: sólo hay que cifrar los datos
- El **cifrado simétrico** es el apropiado para cifrar / descifrar grandes cantidades de información
 - ambos extremos deben conocer la clave de cifrado
- Así pues, basta con elegir un algoritmo de cifrado y ponerse de acuerdo en la clave a utilizar
 - ya veremos el problema de comunicar la clave...
- Los algoritmos pueden funcionar en modo bloque o en modo flujo de datos, teniendo disponibles:
 - bloque: DES, 3DES, AES, Camellia, SEED, ARIA
 - flujo: RC4

Confidencialidad: a tener en cuenta

- La seguridad del cifrado simétrico se basa en la clave: en su tamaño y en que se mantenga secreta
- Toda clave cuyo tamaño sea inferior a **128 bits** se considera débil
 - en otro caso, los ataques por fuerza bruta son efectivos
 - esto descarta DES y “3DES mal implementado”
- Los algoritmos por bloques pueden trabajar en distintos modos: ECB, CBC, OFB, ...
 - ECB no es apropiado -> no se utiliza
 - CBC es vulnerable en SSLv3 / TLS 1.0 (no en TLS 1.1+)
BEAST (CVE-2011-3389)
“Browser Exploit Against SSL/TLS”
Juliano Rizzo, Thai Duong; ekoparty 2011

Confidencialidad: ejemplo (1/2)

Qualys SSL Labs - Projects x

https://www.ssllabs.com/ssltest/analyze.html?d=gestion-servicios.ehu.es&hideResults=on

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3.0	Yes
SSL 2.0 INSECURE	Yes

Cipher Suites (sorted by strength; server has no preference)

SSL_RC4_128_EXPORT40_WITH_MD5 (0x20080) WEAK	40
SSL_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) WEAK	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) WEAK	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) WEAK	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) WEAK	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits (p: 64, g: 1, Ys: 64) WEAK	40
SSL_DES_64_CBC_WITH_MD5 (0x60040) WEAK	56
TLS_RSA_WITH_DES_CBC_SHA (0x9) WEAK	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128) WEAK	56
SSL_RC4_128_WITH_MD5 (0x10080)	128
SSL_RC2_128_CBC_WITH_MD5 (0x30080)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128

Confidencialidad: ejemplo (2/2)

The screenshot displays the Qualys SSL Labs interface. On the left, a sidebar lists protocols and cipher suites. The main content area shows a list of cipher suites with their respective security scores. Below this, a 'Protocol Details' section provides information on various security features.

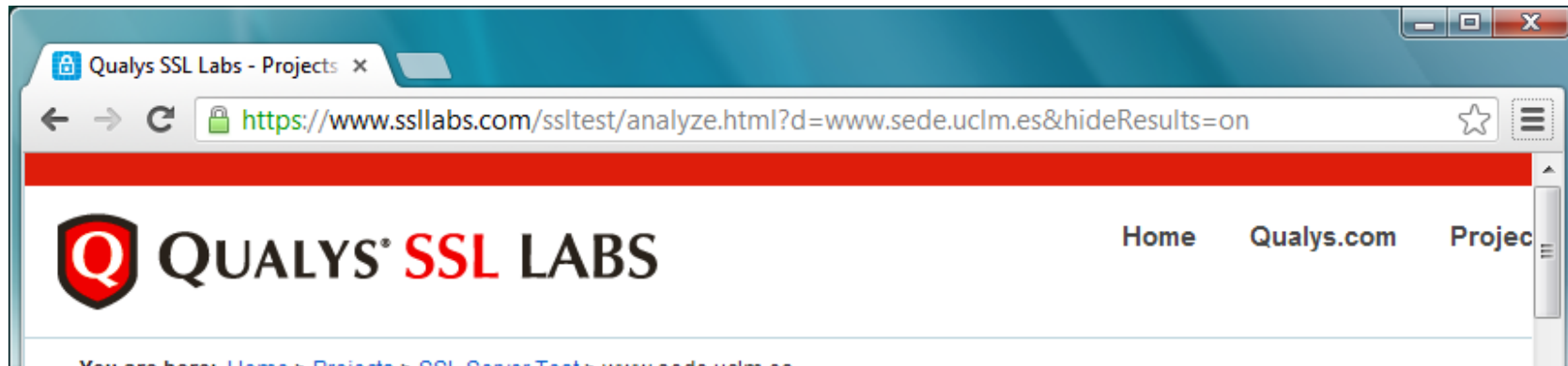
Cipher Suite	Score
TLS_RSA_WITH_DES_CBC_SHA (0x9)	WEAK 50
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128)	WEAK 56
SSL_RC4_128_WITH_MD5 (0x10080)	128
SSL_RC2_128_CBC_WITH_MD5 (0x30080)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128)	128
SSL_DES_192_EDE3_CBC_WITH_MD5 (0x700c0)	168
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128)	168
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128)	256

Feature	Status
Secure Renegotiation	Not supported ACTION NEEDED (more info)
Insecure Renegotiation	Not supported
BEAST attack	Vulnerable INSECURE (more info)
Compression	No
Next Protocol Negotiation	No
Session resumption	Yes

Confidencialidad: compresión

- En la ekoparty 2012, Juliano Rizzo y Thai Duong, nos sorprenden con la puesta en marcha de otro ataque (conocido pero etiquetado como teórico):
 - **CRIME** (*Compression Ratio Info-leak Made Easy*)
- El problema se presenta si utilizamos compresión (si se utiliza es antes del cifrado, claro)
 - en ese caso corremos el riesgo de fuga de información
- Google estaba trabajando seriamente en la mejora del rendimiento de HTTP y la compresión era un mecanismo fundamental
 - a raíz de este ataque se han visto obligados a eliminar la compresión en SSL

Compresión: ejemplo



BEAST attack	Vulnerable INSECURE (more info)
Compression	Yes INSECURE (more info)
Next Protocol Negotiation	No
Session resumption	No (IDs empty)

Integridad

- Puede parecer que habiendo cifrado no es necesario implementar ningún mecanismo de integridad
- Pero existen ataques (de truncamiento, por ejemplo) que exigen garantizar la integridad de los mensajes
- Como es habitual, la integridad se verifica mediante un resumen (*hash*) del mensaje
- Para ello se utiliza la función **MD5** o alguna variante de **SHA** (SHA-1, SHA-256, SHA-384, SHA-512)
- Estas funciones se utilizan con el mecanismo **HMAC**, que utiliza claves secretas al calcular el resumen
- Para cada registro SSL se genera su HMAC antes de ser cifrado

Disponibilidad

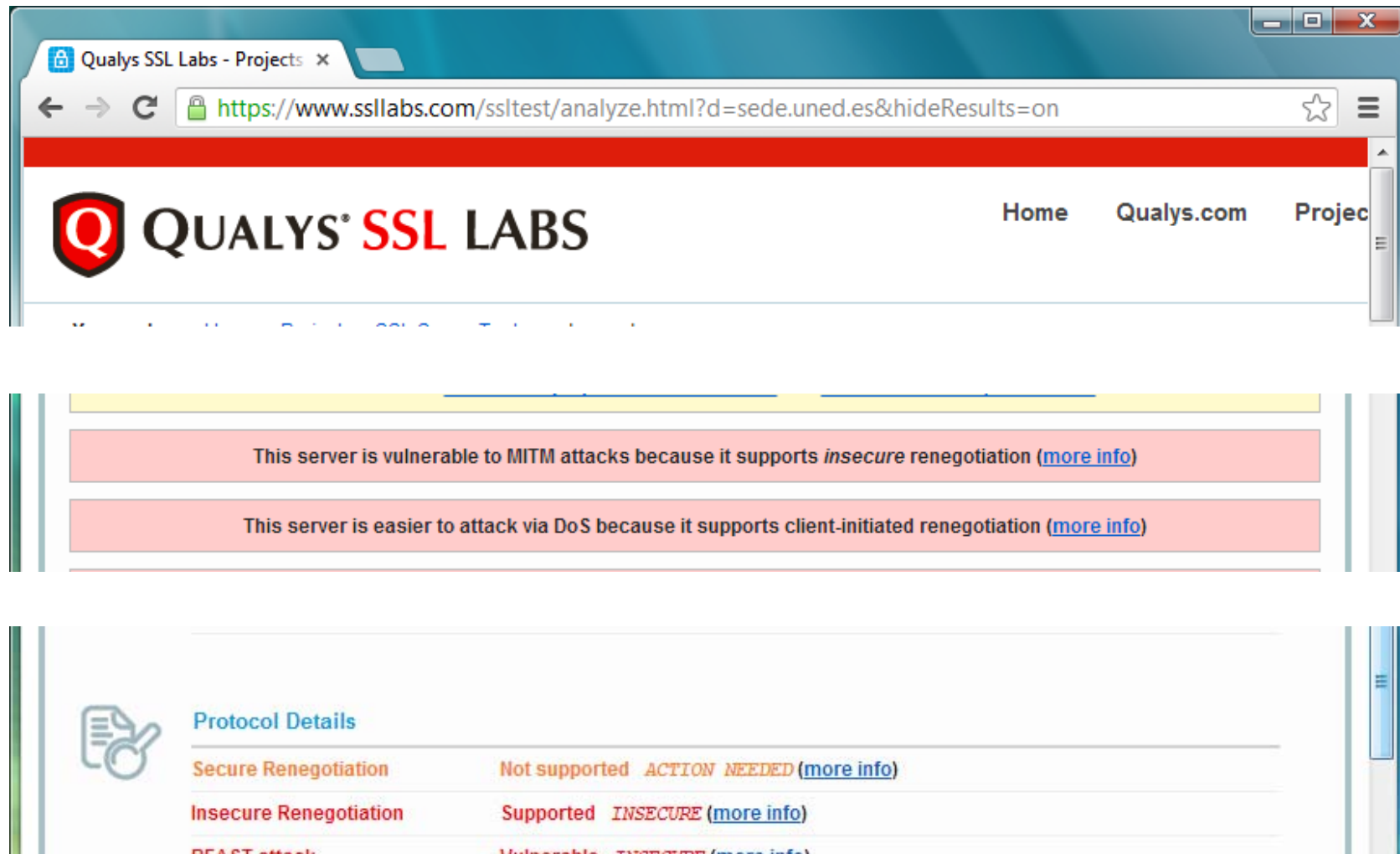
- Está muy extendida la idea de que el uso de SSL consume muchos recursos
- Pero Google (como empresa, no como buscador) no está de acuerdo:
 - <http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html>
 - <http://www.imperialviolet.org/2011/02/06/stillinexpensive.html>
- Y ya que tenemos recursos suficientes para utilizar SSL en todas las conexiones:
 - **Always On SSL**
Online Trust Alliance
<https://otalliance.org/resources/AOSSL/>



Disponibilidad: denegación de servicio

- Si nuestro servidor permite la renegociación SSL iniciada por el cliente, somos vulnerables a ataques de **DoS** (*Denial Of Service*)
- Actualmente se considera que la renegociación sólo debería iniciarla el servidor
- Además, en 2009 se descubrió un fallo de diseño que permitía aprovechar la renegociación para inyectar tráfico en una sesión SSL
 - <https://community.qualys.com/blogs/securitylabs/2009/11/05/ssl-and-tls-authentication-gap-vulnerability-discovered>
- Así pues, nuestros servidores deberían implementar el **RFC 5746**, que soluciona el fallo descrito

Disponibilidad: ejemplo 1



The screenshot shows the Qualys SSL Labs interface for the domain `sede.uned.es`. The browser address bar displays the URL `https://www.ssllabs.com/ssltest/analyze.html?d=sede.uned.es&hideResults=on`. The page header includes the Qualys SSL Labs logo and navigation links for Home, Qualys.com, and Projects.

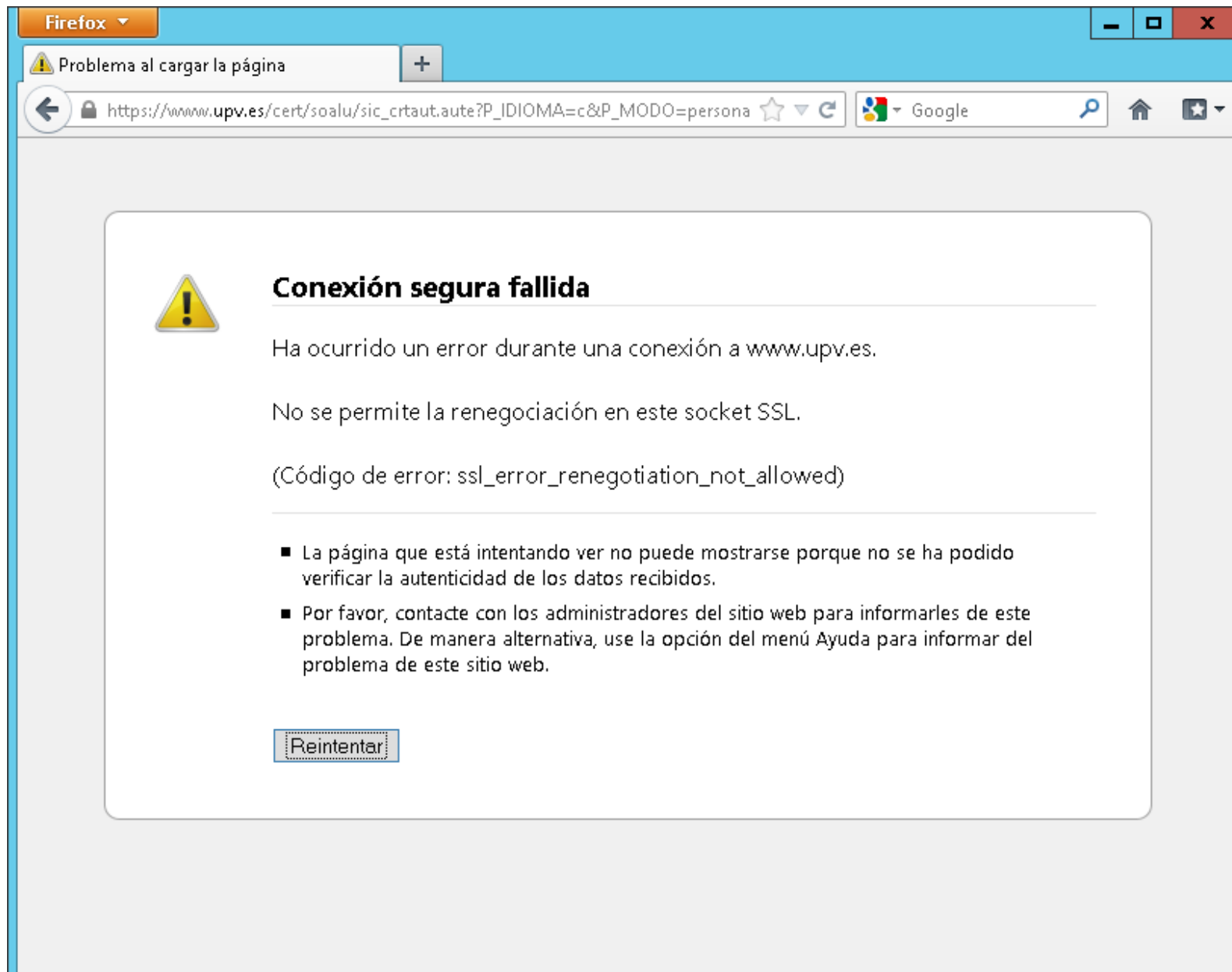
Two prominent red warning boxes highlight the following vulnerabilities:

- This server is vulnerable to MITM attacks because it supports *insecure* renegotiation ([more info](#))
- This server is easier to attack via DoS because it supports client-initiated renegotiation ([more info](#))

The "Protocol Details" section provides a summary of the server's SSL/TLS configuration:

Protocol	Status	Action	More Info
Secure Renegotiation	Not supported	ACTION NEEDED	more info
Insecure Renegotiation	Supported	INSECURE	more info
BEAST attack	Vulnerable	INSECURE	more info

Disponibilidad: ejemplo 2



Autenticidad

- Para comprobar la autenticidad del servidor se utilizan **certificados digitales**: asociación entre una **clave pública** y los **datos de identificación** avalada por un **tercero** de confianza
 - también se pueden utilizar certificados digitales para autenticar al cliente, aunque no es muy habitual todavía
- En general se utiliza **RSA** para gestionar y utilizar el par de claves (una pública y una privada)
 - basado en la complejidad de factorizar en números primos
- Pero veremos aparecer las curvas elípticas en breve
- Los certificados digitales son el origen de la mayoría de problemas que salen a la superficie en SSL

Certificados digitales

- A la hora de obtener un certificado digital tenemos que tomar unas cuantas decisiones:
 - el tamaño de las claves
 - la identificación asociada a la clave pública
 - la entidad raíz a la que solicitamos el certificado
 - el período de validez
 - el tipo de certificado
- Un “mal” certificado puede ponernos las cosas muy difíciles para generar confianza en los usuarios
 - por decirlo de manera suave...
- Un “buen” certificado no es suficiente para que SSL funcione bien (automáticamente)

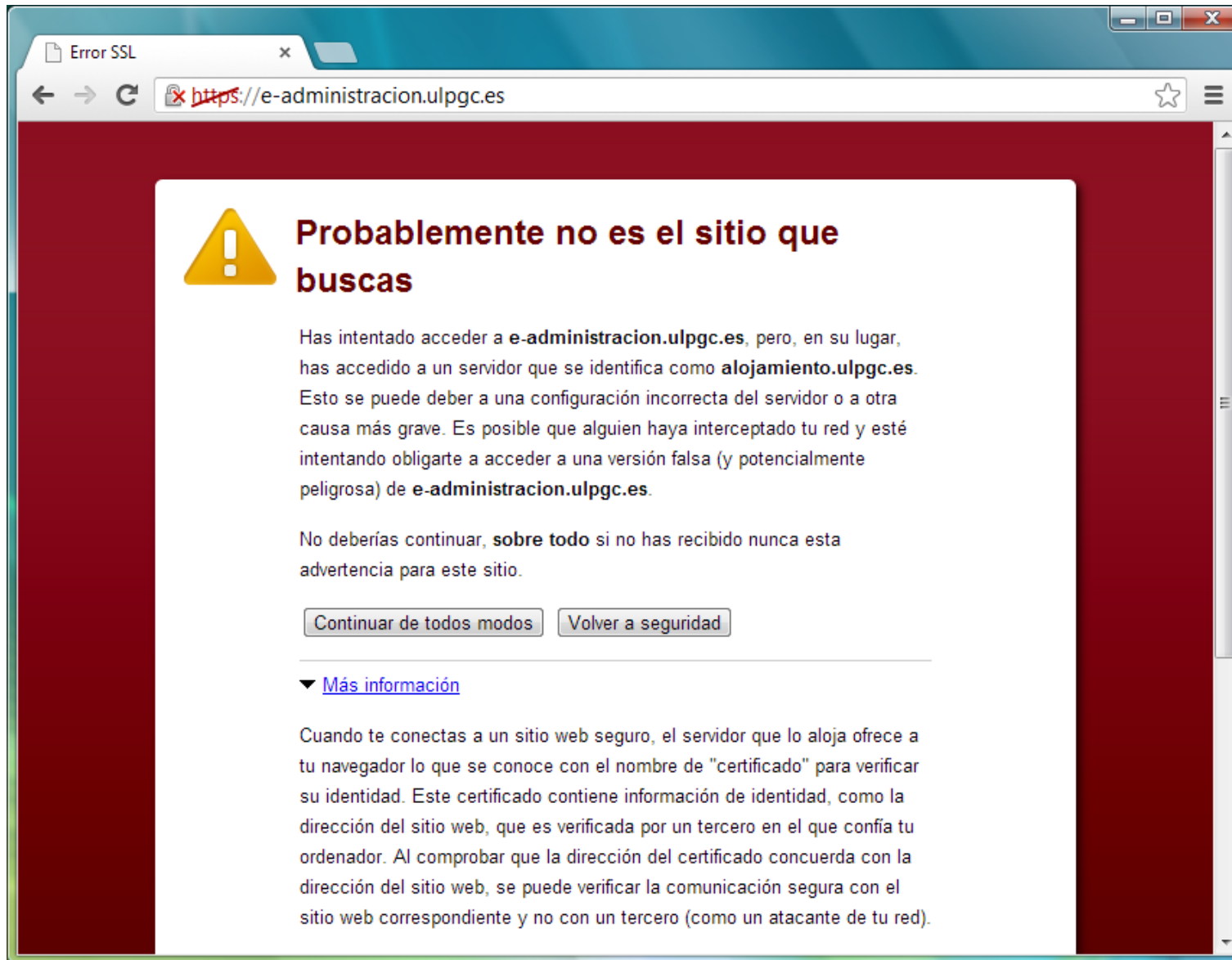
Certificados digitales: claves

- Las claves de cifrado asimétrico tienen un tamaño mucho mayor que las claves de cifrado simétrico
- El mínimo exigible para RSA es de 1024 bits
- Aunque el mínimo recomendable es de **2048 bits**
 - romper una clave asimétrica de 2048 bits es equivalente a romper una clave simétrica de 112 bits
- Cuanto más tiempo utilicemos las mismas claves, más tiempo daremos para averiguarlas
- Se recomienda utilizar claves asimétricas sólo durante un año y generar nuevas con cada renovación del certificado
 - se desaconseja completamente utilizarlas más de 3 años

Certificados digitales: identificación

- Cuando un usuario se conecta a un servidor utiliza un nombre DNS para localizarlo
- En nuestro certificado tendremos que asociar la clave pública a **todos los nombres** que pueden utilizar los usuarios para llegar a nuestro servidor
- Podría ser que sólo tuviésemos un nombre posible
 - aparecería como CN dentro del atributo **Subject**
- Que tuviésemos varios nombres alternativos
 - aparecerían en el atributo **SubjectAlternativeName** (y, en dicho caso, el atributo Subject se ignora)
- Que utilicemos un comodín (como prefijo) para agrupar todos los nombres de un subdominio

Identificación: ejemplo (1/2)



Identificación: ejemplo (2/2)

The image shows a web browser window with the address bar displaying `https://e-administracion.ulpgc.es`. The page content includes a yellow warning triangle icon and the text "Probablemente no es el sitio que buscas".

Two "Certificado" (Certificate) dialog boxes are overlaid on the browser window. The left dialog shows the "General" tab with the following information:

- Información del certificado**
- Este certificado está destinado a los siguientes propósito:
 - Asegura la identidad de un equipo remoto
 - Prueba su identidad a un equipo remoto
- Emitido por: alojamiento.ulpgc.es
- Emitido por: TERENA SSL CA
- Válido desde: 14/10/2010 hasta: 14/10/2013

The right dialog shows the "General" tab with a table of certificate fields:

Campo	Valor
Puntos de distribución CRL	[1]Punto de distribución CRL: ...
Acceso a la información de ...	[1]Acceso a información de au...
Nombre alternativo del sujeto	Nombre DNS=alojamiento.ulpg...
Uso de la clave	Firma digital, Cifrado de clave ...
Restricciones básicas	Tipo de asunto=Entidad final, ...
Algoritmo de identificación	sha1
Huella digital	fe 20 ef 12 a7 cc ef bc 2b 55 3...

Below the table, the following DNS names are listed:

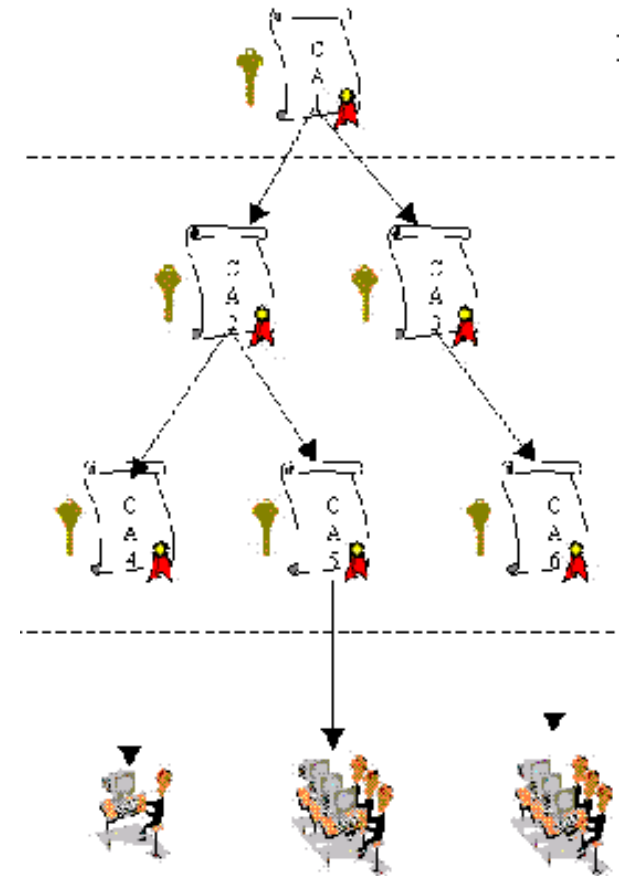
- Nombre DNS=alojamiento.ulpgc.es
- Nombre DNS=autorizacion.ulpgc.es
- Nombre DNS=biblioteca.ulpgc.es
- Nombre DNS=desarrollobu.ulpgc.es
- Nombre DNS=ftpactasssl.ulpgc.es
- Nombre DNS=preproduccionbu.ulpgc.es

Certificados digitales: entidad raíz

- La asociación entre clave pública e identificación la firma una entidad certificadora (CA)
- Para que los clientes confíen en el certificado tienen que confiar, previamente, en dicha entidad
- En un entorno controlado podríamos utilizar nuestra propia CA y distribuirla a todos nuestros clientes
 - ¿existe dicho entorno?
- La opción más adecuada es utilizar una de las entidades raíz que estén distribuidas ampliamente
 - en la mayoría de navegadores y dispositivos
- RedIRIS nos proporciona gratuitamente certificados firmados por la CA de Comodo (actualmente)

Certificados digitales: jerarquía

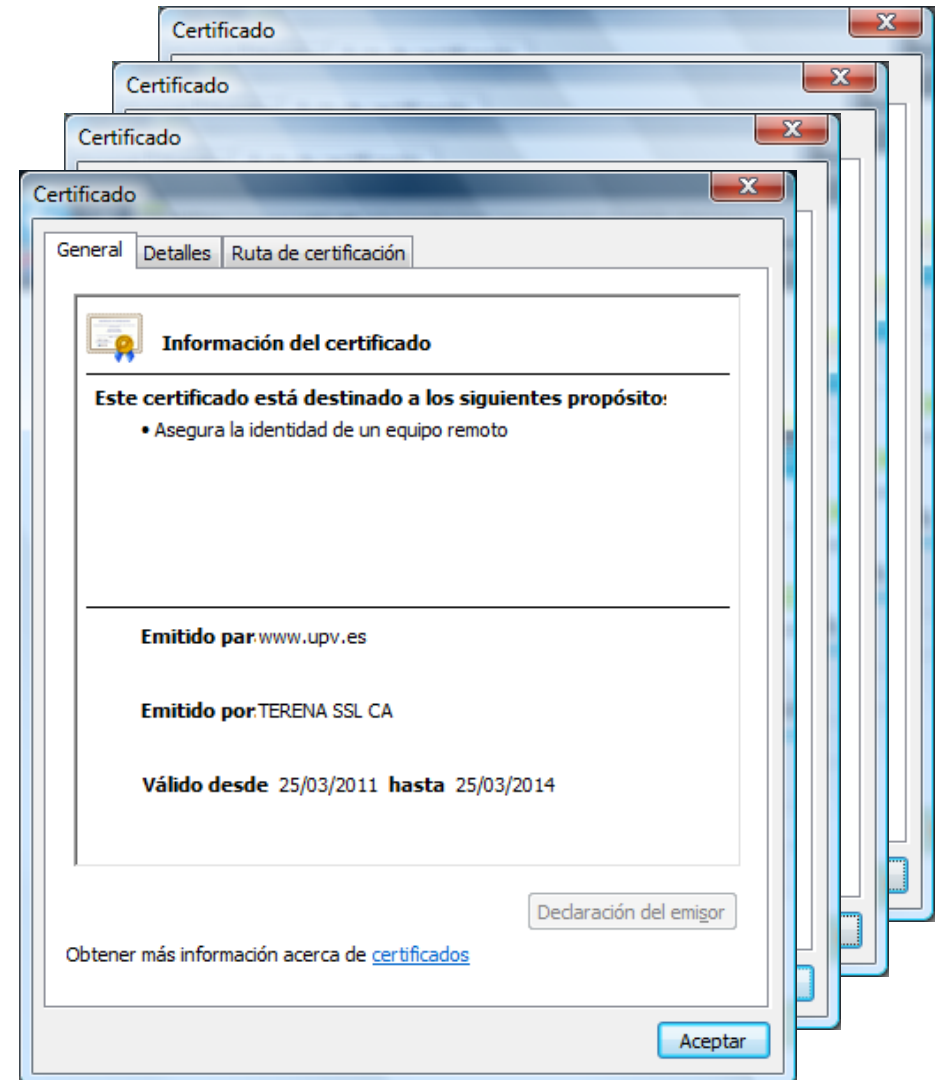
- Las autoridades de certificación utilizan una jerarquía de entidades, de manera que la entidad raíz sólo firma a otras entidades certificadoras
- Los clientes sólo necesitan confiar en las entidades raíz, nunca es necesario que instalen entidades intermedias
- No entregar los certificados de las entidades intermedias es uno de los errores más frecuentes
 - además, no se puede verificar “probando” que funciona



Jerarquía de certificados (1/6)

cliente

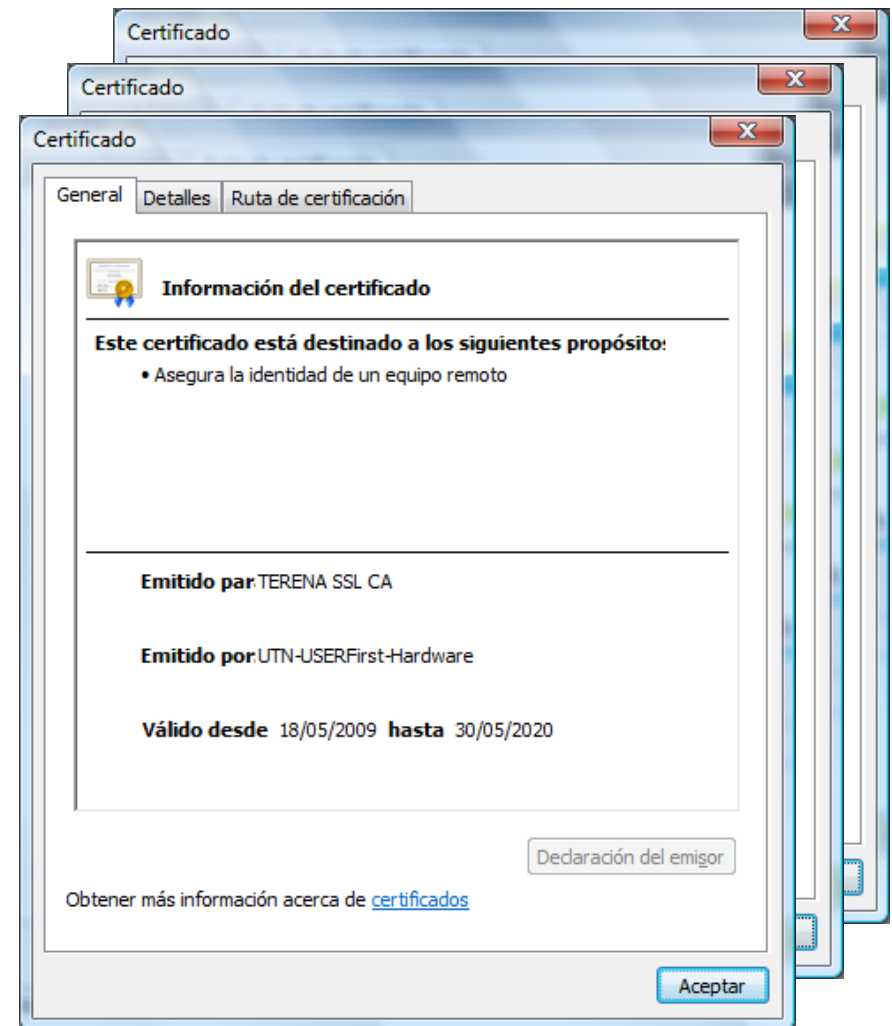
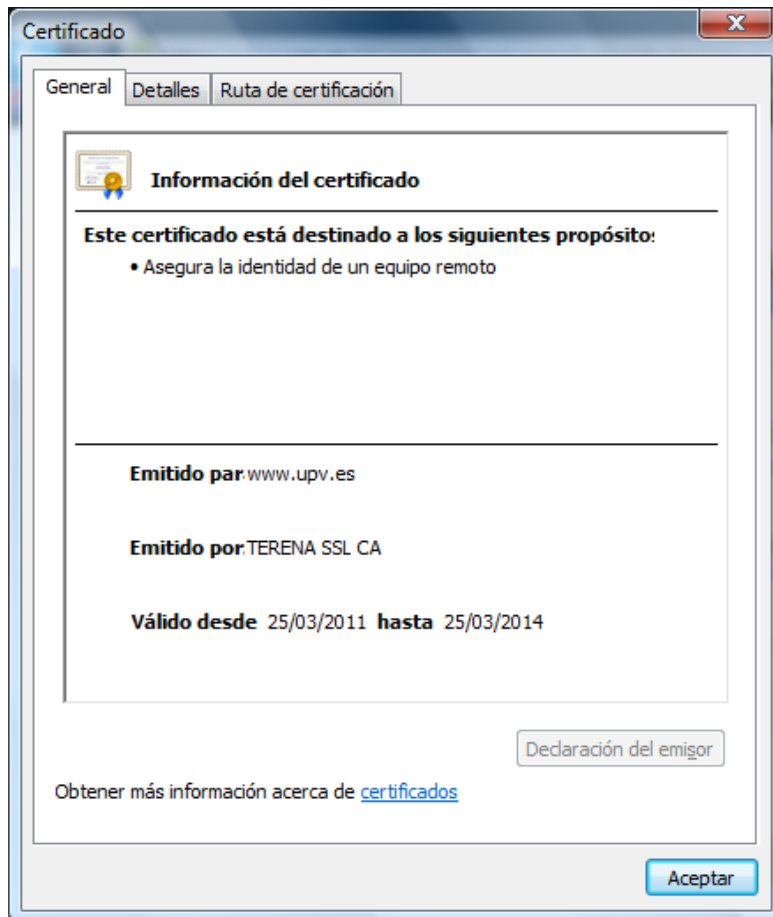
servidor



Jerarquía de certificados (2/6)

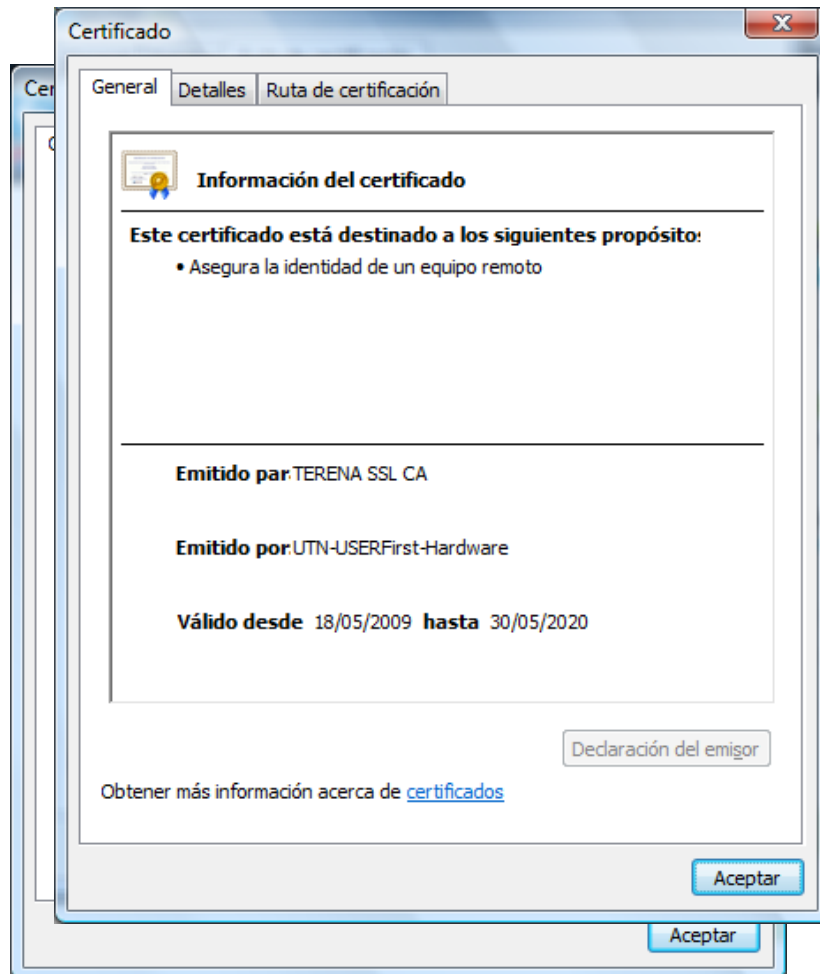
cliente

servidor

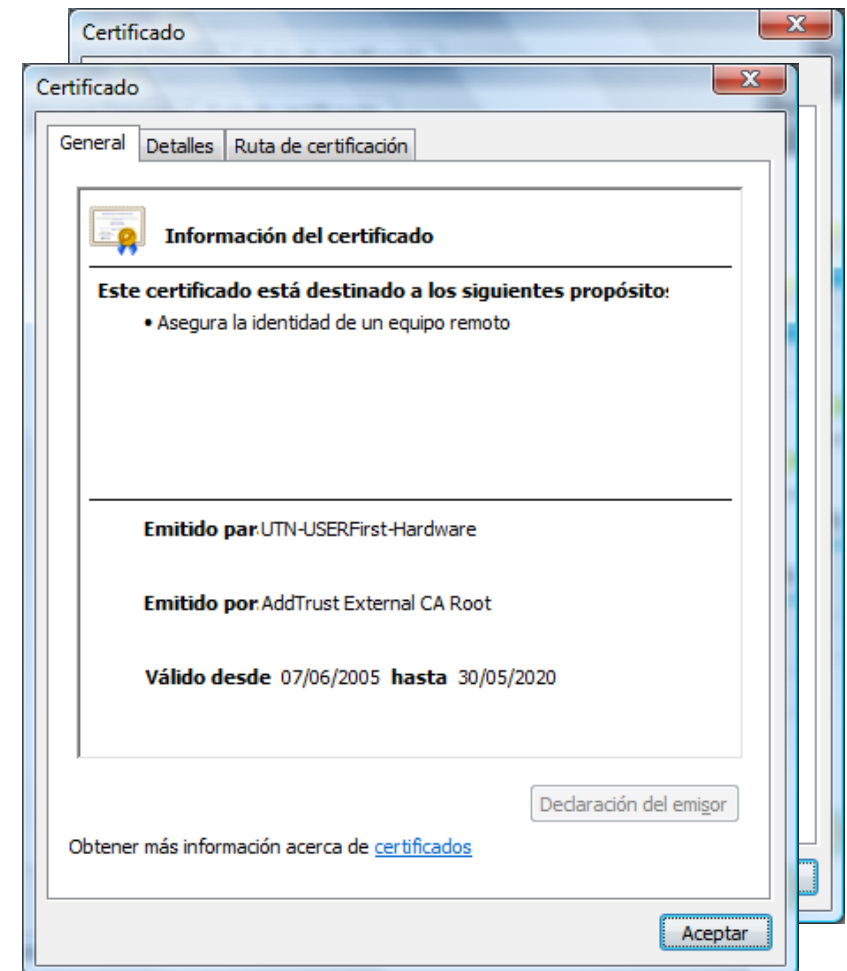


Jerarquía de certificados (3/6)

cliente

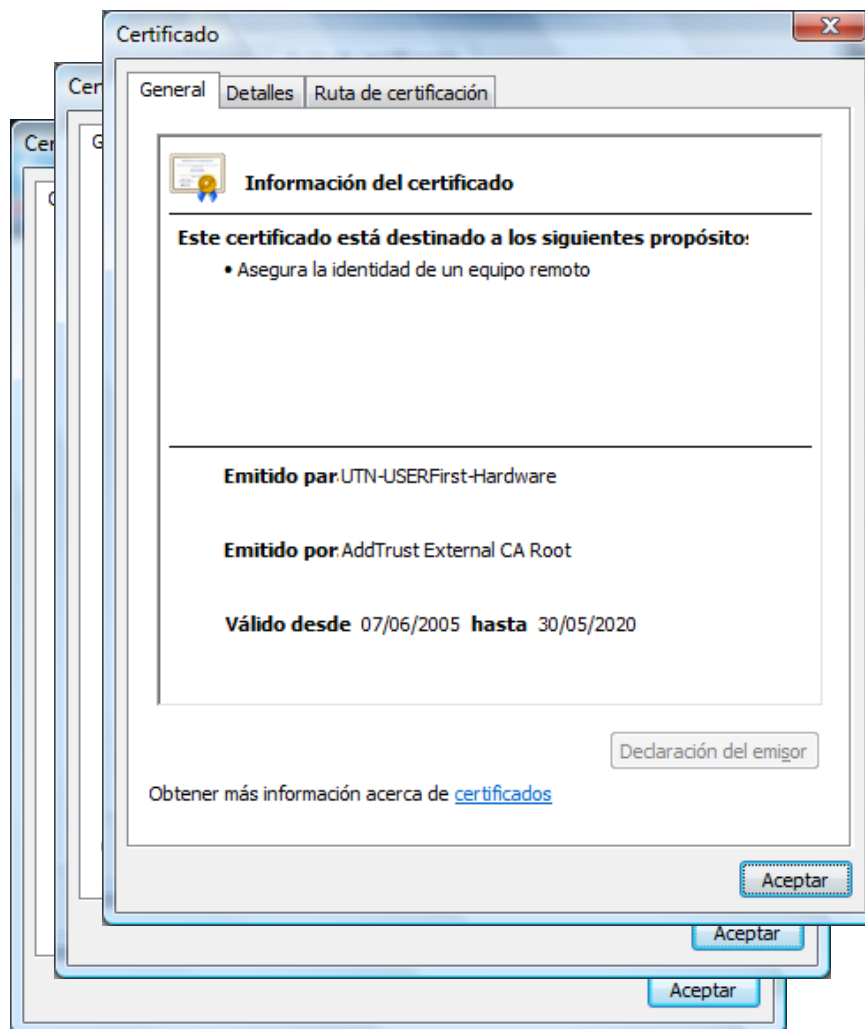


servidor

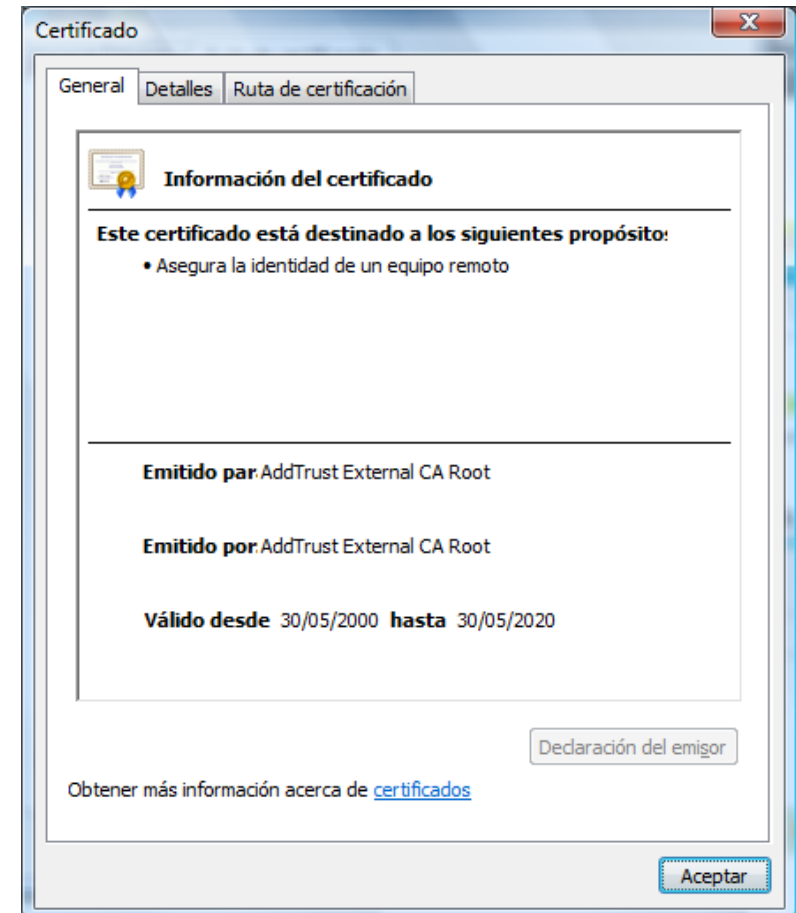


Jerarquía de certificados (4/6)

cliente



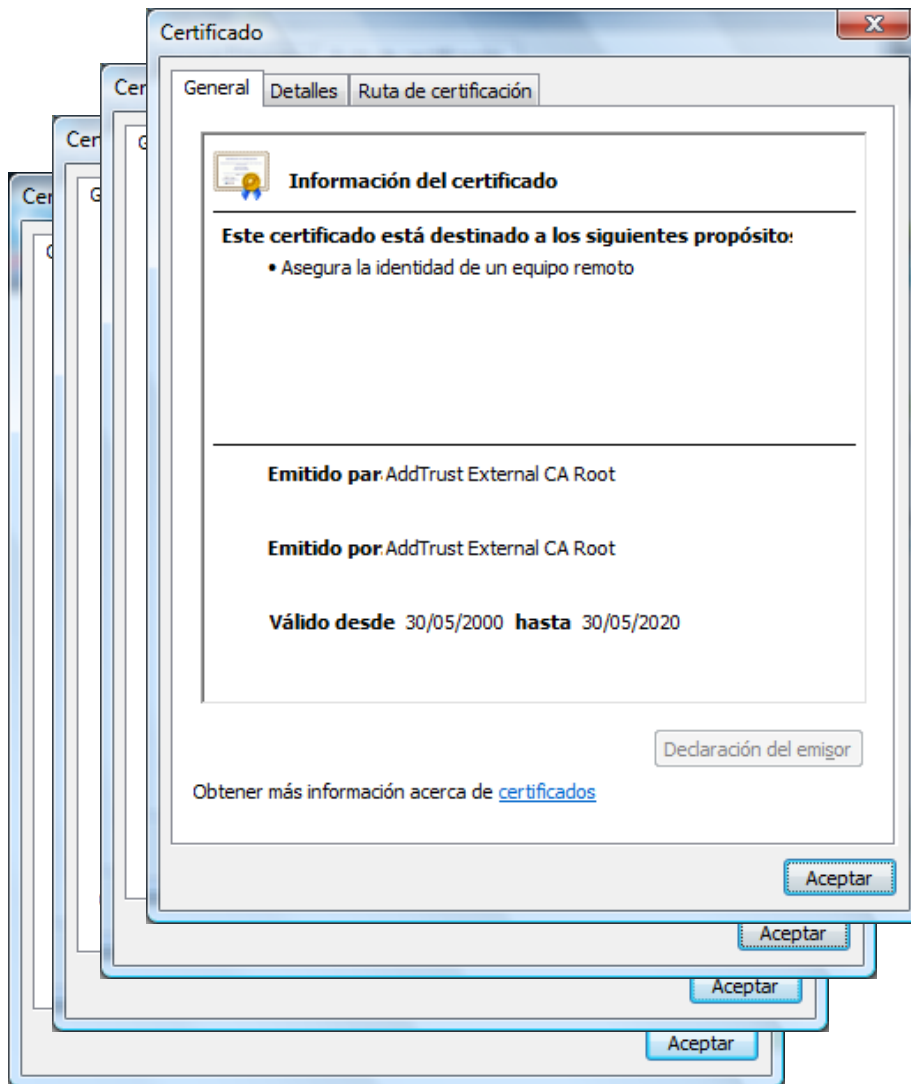
servidor



Jerarquía de certificados (5/6)

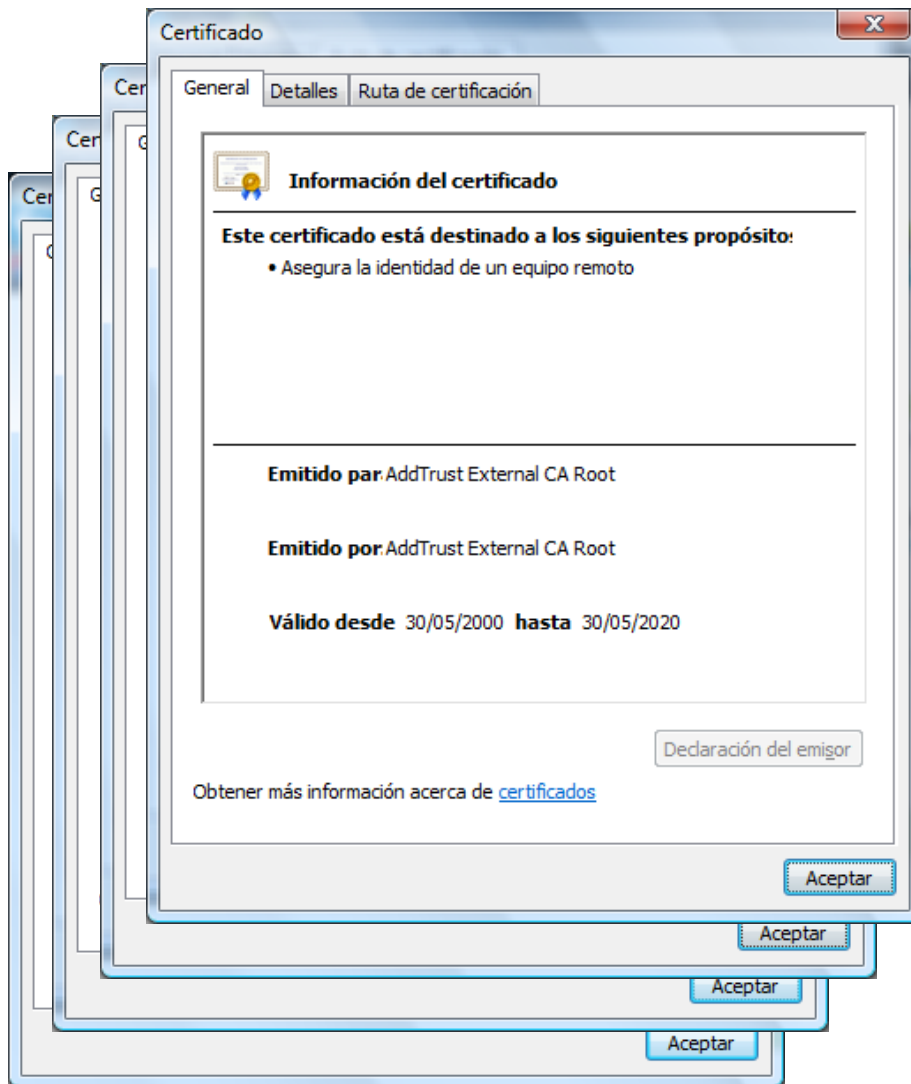
cliente

servidor

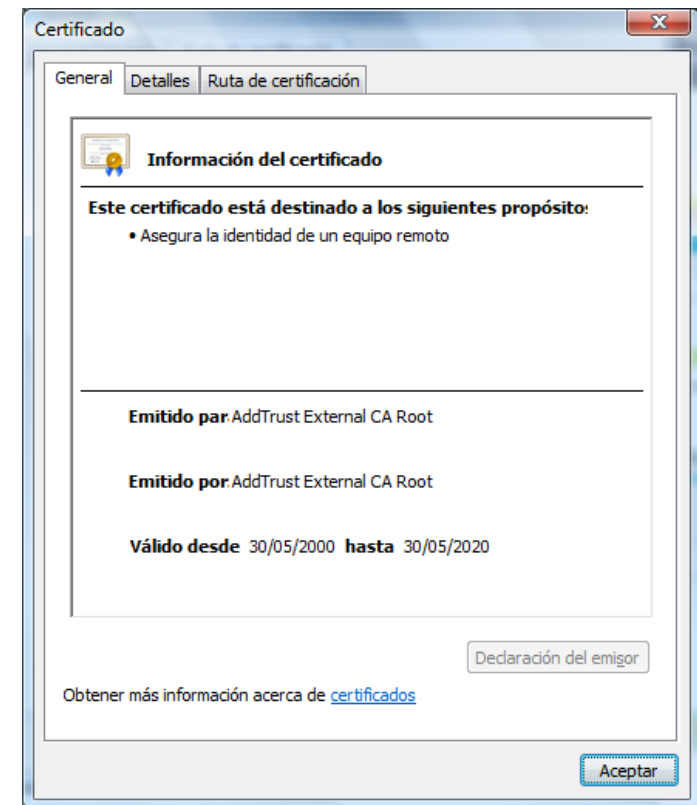


Jerarquía de certificados (6/6)

cliente



CA raíz de confianza



Cadena errónea: ejemplo

```
>openssl s_client -connect www.sede.uclm.es:443
```

```
...
```

```
Certificate chain
```

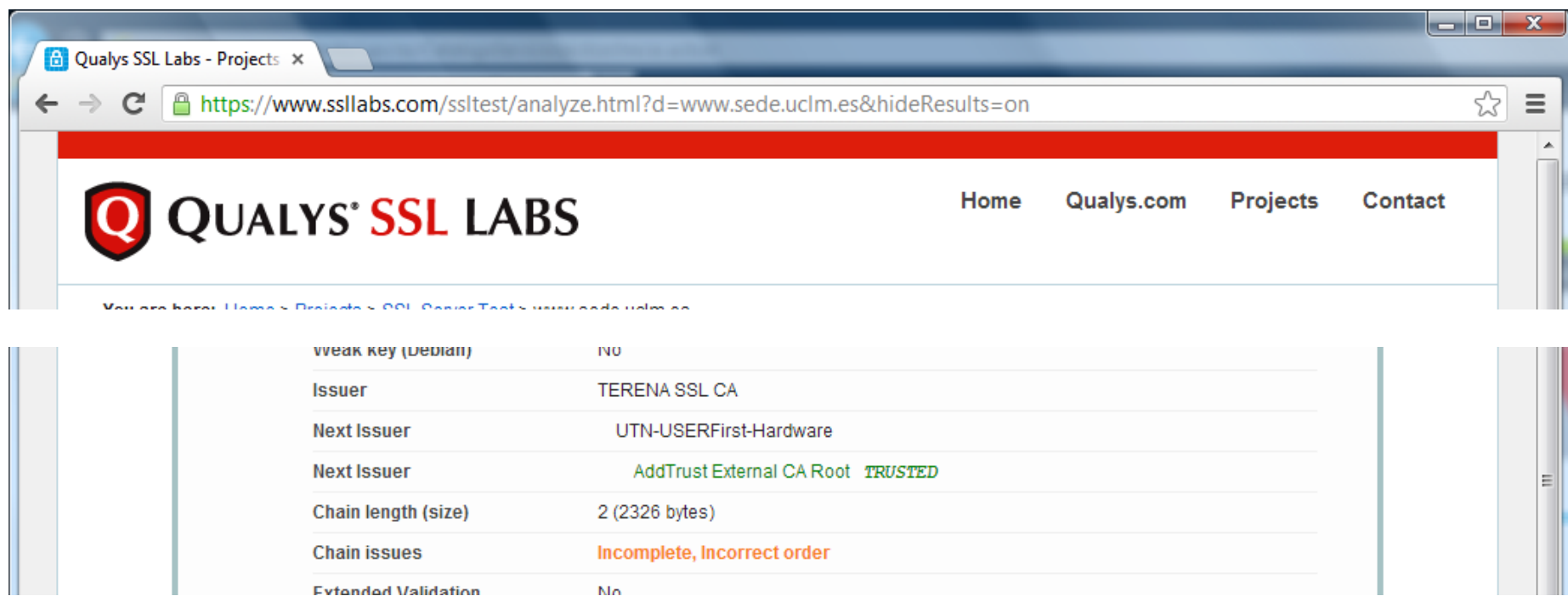
```
0 s:/C=ES/ST=Castilla-La Mancha/L=Castilla-La Mancha/O=Universidad de Castilla-La Mancha - Q1368009E/OU=uclm.es/CN=www.sede.uclm.es
```

```
i:/C=NL/O=TERENA/CN=TERENA SSL CA
```

```
1 s:/C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware
```

```
i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
```

```
...
```



Qualys SSL Labs - Projects

https://www.ssllabs.com/ssltest/analyze.html?d=www.sede.uclm.es&hideResults=on

Home Qualys.com Projects Contact

QUALYS[®] SSL LABS

You are here: Home > Projects > SSL Server Tests > www.sede.uclm.es

Weak key (Default)	No
Issuer	TERENA SSL CA
Next Issuer	UTN-USERFirst-Hardware
Next Issuer	AddTrust External CA Root TRUSTED
Chain length (size)	2 (2326 bytes)
Chain issues	Incomplete, Incorrect order
Extended Validation	No

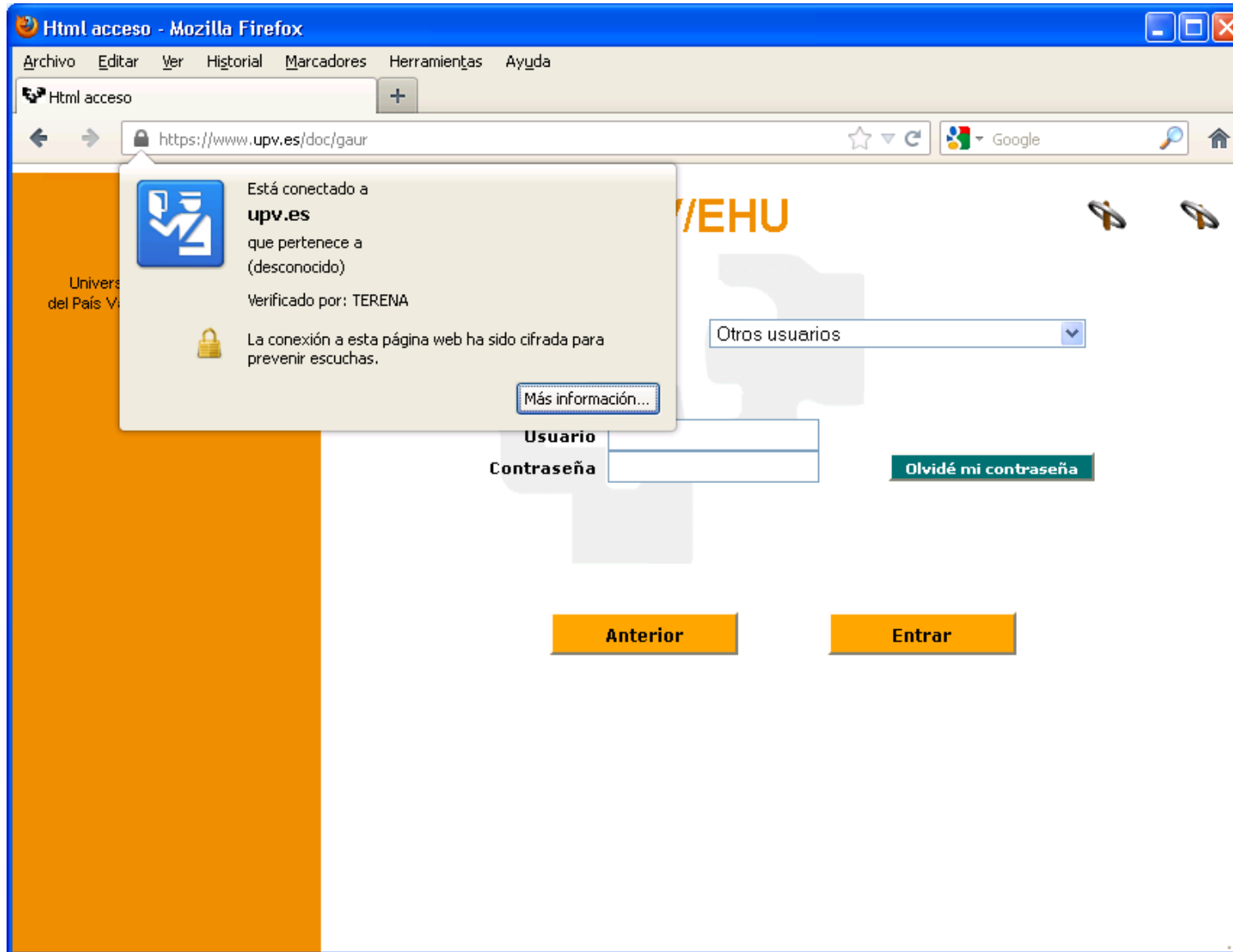
Certificados digitales: tipo

- Los certificados digitales establecen el **uso** que se puede dar a las claves y los **datos** identificativos que se muestran sobre el propietario
- También hay distintas opciones en cuanto a las comprobaciones que hace una CA sobre los datos
- Esto da lugar a distintos tipos de certificados:
 - clase 1 / *domain validation*
 - clase 2 / *organization verified*
 - *extended validation* (EV)
 - de sede electrónica
- Para el usuario sólo hay 2 tipos: el “verde” (EV) y todos los demás

Certificados EV: ejemplo (1/4)

The screenshot shows a Mozilla Firefox browser window with the title "Html acceso - Mozilla Firefox". The address bar displays "https://www.upv.es/doc/gaur". The page content includes the UPV/EHU logo and the text "Universidad del País Vasco Euskal Herriko Unibertsitatea". A navigation menu on the left lists "GAUR". The main content area features a login form with a dropdown menu labeled "Universitarios" and "Otros usuarios", input fields for "Usuario" and "Contraseña", a "Olvidé mi contraseña" button, and "Anterior" and "Entrar" buttons.

Certificados EV: ejemplo (2/4)



Certificados EV: ejemplo (3/4)

The screenshot shows a Mozilla Firefox browser window displaying the identification page of the Universitat Politècnica de València (UPV). The browser's address bar shows the URL `https://intranet.upv.es/pls/soalu/est_intranet.NI_Dual?P_IC`. The page features the UPV logo and a navigation menu with categories like Idioma, Tipografía, Estudios, Investigación, Organización, and Otros. The main heading is "Identificación UPV. Accediendo a Intranet".

There are two main login sections:

- Identificación como alumno de la UPV:** Includes input fields for "DNI (x)" and "PIN (x)", and an "Entrar" button.
- Identificación como personal o externo en la UPV:** Includes radio buttons for "Intranet" (selected) and "Extranet", input fields for "DNI (x)" and "Clave UPVnet (x)", and an "Entrar" button.

Below these sections are two boxes for "Acceso con certificado". Each box contains the text: "Ahora ya puedes acceder a la intranet identificándote mediante el DNI-Electrónico o el certificado digital de la GVA. [Más información](#)". Below this text is an "Entrar" button and a small image of a digital certificate card. The second box also includes the instruction: "Para poder acceder con certificado introduce tu tarjeta en el lector y pulsa".

Certificados EV: ejemplo (4/4)

Html acceso - Mozilla Firefox

Identificación UPV. Accediendo a Intranet - Mozilla Firefox

Identificación UPV. Accediendo a Intranet

Universitat Politècnica de València (ES) https://intranet.upv.es/pls/soalu/est_intranet.NI_Dual?P_IC

Está conectado a **upv.es** que pertenece a **Universitat Politècnica de València** Valencia Comunitat Valenciana, ES Verificado por: COMODO CA Limited

La conexión a esta página web ha sido cifrada para prevenir escuchas.

Más información...

Identificación como alumno de la UPV

Identificación como personal o externo en la UPV

Acceso a Intranet Extranet

DNI (*)

PIN (*)

Entrar

Entrar

Acceso con certificado

Ahora ya puedes acceder a la intranet identificándote mediante el DNI-Electrónico o el certificado digital de la GVA. [Más información](#)

Para poder acceder con certificado introduce tu tarjeta en el lector y pulsa **Entrar**

Entrar

Certificados: validación

- Para validar un certificado hay que comprobar que:
 - el nombre que utilizamos coincide con uno de los nombres incluidos en el certificado
 - el certificado se encuentra vigente
 - el certificado no ha sido revocado
- Éstas comprobaciones se tienen que hacer para el certificado del servidor y para los certificados de todas las entidades intermedias
- La revocación se puede consultar a través de listas **CRL** o utilizando un servicio **OCSP**
- Hablando de la FNMT: ¿qué pasaría si te roban la clave privada de tu certificado?

Certificados: OCSP

- Comprobar la revocación es fundamental para confiar en un certificado
- OCSP mejora el rendimiento de las CRL, pero ha tenido y sigue teniendo algunos problemas
 - por ejemplo, de privacidad: cada vez que visitamos un sitio web se lo “decimos” a la CA de su certificado
- La extensión de TLS **Status Request** (conocida como **OCSP stapling**: grapado OCSP) es perfecta:
 - el cliente solicita al servidor (en el establecimiento del túnel SSL) que le informe del estado de revocación de su certificado
 - es el servidor, por tanto, el encargado de hacer las consultas OCSP

Intercambiando claves simétricas

- Habíamos dejado pendiente un gran problema: ¿cómo nos ponemos de acuerdo para usar una clave secreta (y que siga siendo secreta)?
- El uso de certificados digitales para la autenticación resuelve este problema:
 - la clave simétrica se cifra de manera asimétrica
- Grosso modo: el cliente cifra, con la clave pública del servidor, la clave simétrica y se la envía a éste
- ¿Y si alguien guarda la comunicación cifrada y logra descubrir (o robar) la clave privada del servidor?
- **Secreto permanente** (*perfect forward secrecy*): Diffie-Hellman (EDH) para intercambio de claves

Conjuntos de cifrado

- Para establecer un túnel SSL, cliente y servidor utilizan descriptores (*cipher suites*) para ponerse de acuerdo en los siguientes elementos:
 - algoritmo de intercambio de clave
 - algoritmo de cifrado
 - algoritmo de resumen (hash)
- Ejemplos:
 - TLS_RSA_WITH_AES_128_CBC_SHA256
 - TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- Puedes consultar el listado completo en:
 - <http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-3>

Sitios web: un caso especial

- Las características de la web hacen que SSL no sea suficiente para garantizar las comunicaciones:
 - si consiguen robar nuestras cookies podrán suplantarnos (aunque tengamos perfectamente configurado SSL)
- Además de desarrollar la web con la seguridad en mente, hay que tener cuidado de:
 - marcar las *cookies* de sesión con los atributos **Secure** (sólo se transmitirán por HTTPS) y **HTTPOnly** (no serán accesibles desde JavaScript)
 - no utilizar contenido mixto (elementos servidos por HTTPS y por HTTP en la misma página)
 - es un error tremendamente frecuente
- Es imprescindible, también, el uso de **HSTS**

Contenido mixto: ejemplo

The image shows a web browser window with a mixed content warning. The address bar displays a URL with a red 'x' over the 'https' part, indicating that the page contains both secure (https) and non-secure (http) content. The page title is 'RedIRIS - ¿Podemos ayudarte?' and the URL is 'https://www.rediris.es/ayuda/'.

The page content includes:

- Header: 'Conectando la I+D+i española desde 1988' with logos for 'GOBIERNO DE ESPAÑA', 'MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD', 'MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO', 'red.es', and 'Red IRIS'.
- Search bar: 'Buscador Google™ Custom Search'.
- Navigation menu: 'Inicio', 'Ayuda', 'Sobre RedIRIS', 'La Red', 'Servicios', 'Proyectos', 'Actividades', 'Difusión'.
- Section: '¿Podemos ayudarte?' with a text block: 'Este formulario le permitirá ponerse en contacto con RedIRIS. No olvide poner sus datos de contacto (nombre, centro o universidad a la que pertenece, etc) y explique de forma detallada los objetivos de su petición. Su dirección de correos es necesaria para que podamos ponernos en contacto con usted.'
- Form fields: 'Su dirección de correo electrónico', 'Motivo de su consulta:' (dropdown menu with 'Consulta general' selected), 'Asunto', and 'Texto del mensaje'.

The browser's address bar shows a warning icon and the text 'https://www.rediris.es/ayuda/'. The page content is partially obscured by a smaller, semi-transparent version of the same page, illustrating the mixed content issue.

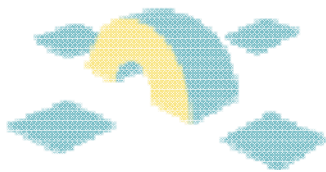
Configurando SSL/TLS

GRACIAS POR

Hacia la seguridad real...

TU ATENCIÓN

Miguel Macías Enguïdanos
miguel.macias@upv.es



IRIS



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

XXXIV Grupos de Trabajo
Bilbao, 27/11/2012

Por cierto...



- Lamentablemente no mencionan **S/MIME** (o, para no asustar a nadie: firmado y cifrado digitales)
- ¿Sabías que RedIRIS nos ofrece SCP?