

Instalación de SSL para un dominio (RAN)

Muy importante: Guardar en sitio seguro toda la información que usamos para generar los certificados:

Guardar la información en srv-datos/proyectos en curso/<nombre del proyecto>/documentos definitivos/SSL/csr.txt

- CSR que generamos desde el servidor.
- El certificado que nos devuelve IPSCA o GODADDY. **Actualmente usamos GODADDY.**

Asignación de IP fija en RAN (SAT)

Asignación de una IP fija para el dominio. En este momento tenemos asignadas 10 IP fijas para el servidor.

Pasos a seguir:

1. Entramos como administrador en RAN, vamos a mostrar cuentas y seleccionamos la cuenta a la que queremos asignarle esa IP.
2. Seleccionamos la opción de “Modificar usuario <nombre_usuario>” en los botones de la parte superior.
- 3a. Cambiamos la IP a la que apunta el dominio en los DNS (sólo en los casos en que el servidor de DNS no sea el nuestro). En caso contrario pasar al punto 3.b.
- 3b. Seleccionamos la IP que queremos asignarle en “Setear IP para”.

Generación de CSR (Jefe de Proyecto)

Entramos como usuario en su panel de control del servidor de RAN para generar el CSR (Petición de creación de certificado).

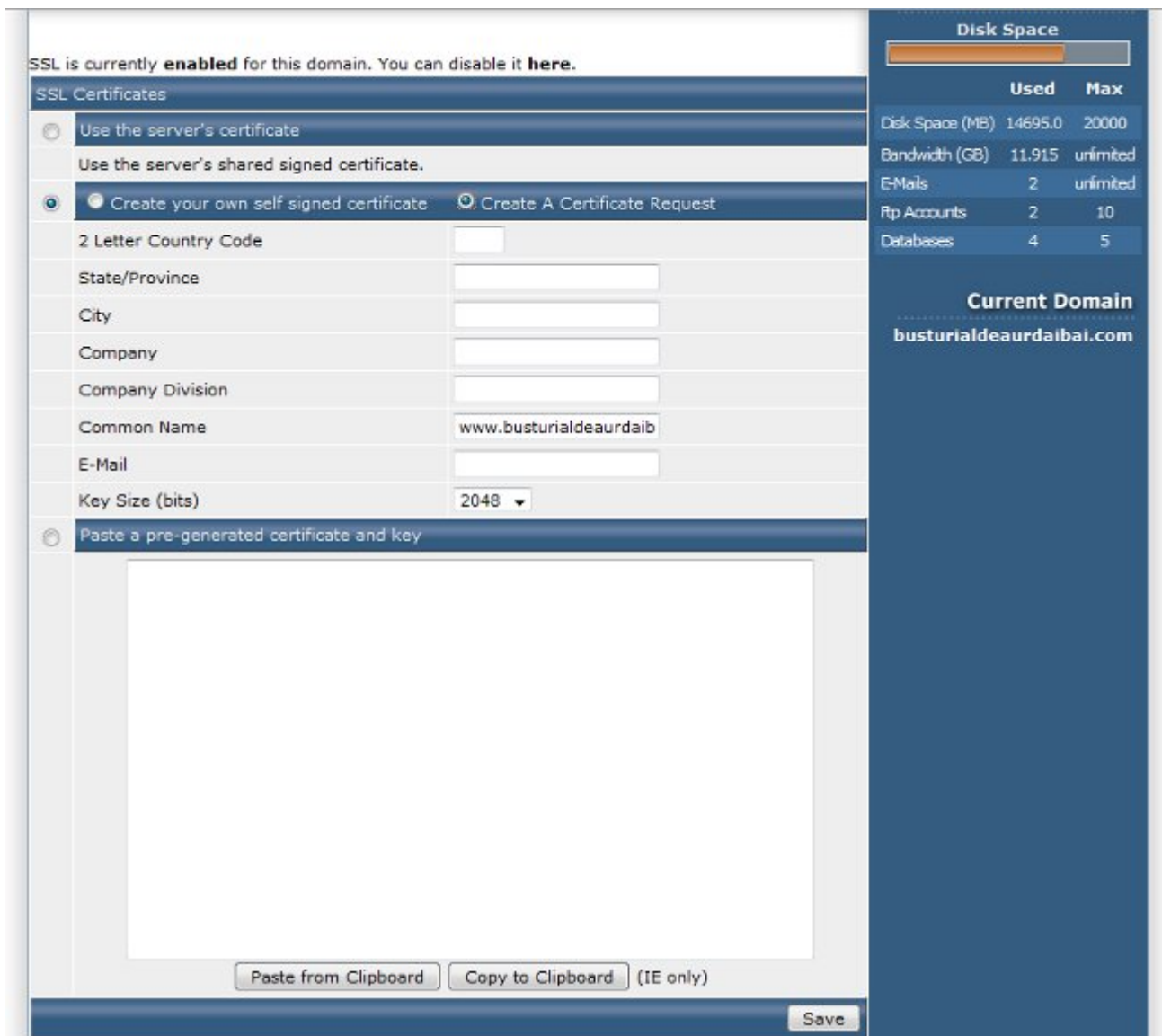
Lo hacemos desde Advanced features → SSL Certificates

Elegimos la opción 2 → Create A Certificate Request

Metemos todos los datos y nos genera el CSR.

- **2 Letter Country Code:** La abreviación ISO del país (p.e. ES)
- **State/Province:** Provincia donde se encuentra la organización (no se puede abreviar) (p.e. Vizcaya)
- **City:** Ciudad donde se encuentra la organización. (p.e. Bilbao)
- **Company:** El nombre legal exacto (p.e. Merkatu Interactiva SL)

- **Company Division:** Departamento de la organización que gestiona el certificado (p.e. Internet)
- **Common Name (Server Host Name):** El dominio de la WEB. Tiene que ser exacto (p.e. www.merkatu.com). Sino se puede recibir un warning.
- **email:** webmaster@merkatu.com. este es el que hay que usar (para poder gestionar nosotros el tema de certificados).
- **ATENCIÓN!!!!!!!!!!!!!!!!!!!!!! el CSR debemos firmarlo con 2048 bits.**



Generación de CSR manual

Ejecutamos los siguientes comandos en el servidor.

→ openssl genrsa -out dominio.com.key 2048

→ openssl req -new -key dominio.com.key -out dominio.com.csr

Con esto generamos el csr y la key para poner luego en el servidor.

Generación de certificado en godaddy.com

Accedemos a la nuestra cuenta de usuario en godaddy.com y procedemos a comprar el/los crédito/s para el certificado seguro.

Una vez hecho esto accedemos a la sección "SSL certificates" dentro del menú "My Account". Aquí usamos el crédito que hemos comprado anteriormente (nos parece en la parte de arriba un enlace llamado "use credit") y le damos a continuar en el botón de la derecha donde nos aparece "Choose from your available credit(s):".

En la lista que nos parece abajo pulsamos en "Manage certificates", accediendo al centro de control de certificados.

Elegimos el disponible y seguimos las instrucciones.

ATENCIÓN!!!!!!!!!!!!!!!!!!!! el CSR debemos firmarlo con 2048 bits.

Generación de certificado en IPSCA **** (OBSOLETO) ****

Aquí tiene los códigos y precios que tienen para cada uno de nuestros certificados de servidor:

Para un dominio:

- 99271166 1 year Merkatu Interactiva S.L.
- 99271178 2 year Merkatu Interactiva S.L.

Certificados para un dominio y todos sus subdominios asociados:

- 99271205 1 year Wildcard Merkatu Interactiva S.L.
- 99271229 2 year Wildcard Merkatu Interactiva S.L.

Certificado Merkatu

Como partner, tienes el derecho a recibir un certificado gratuito para tu dominio, renovado anualmente.

Para obtener el certificado gratuito, realiza una petición de un certificado de 1 año desde nuestra web. Comunícanos a través de este portal el "ticket" de tu petición, indicando en el asunto "Partner realizando la petición del Certificado para Partners", y te enviaremos un e-mail de respuesta para continuar el proceso normal de petición sin necesidad de que realices desembolso alguno.

Certificado para clientes

Pasos a seguir

* Para solicitar certificados para tus clientes basta con que envíes el formulario en <http://certses.ipsca.com/SrvC/Default.htm>. Debes seleccionar "PARTNER" en el tipo de Certificado, introducir tu código y te asignará automáticamente la siguiente lista de precios:

- Certificado de 1 año: €27
- Certificado de 2 años: €49

- Certificado "wildcard" de 1 año: €196
- Certificado "wildcard" de 2 años: €352

Este es el precio que nosotros te facturaremos por los certificados solicitados para tus clientes. Contactaremos directamente contigo para realizar todas las operaciones de autorización, renovación, etc.

NOTA IMPORTANTE:

Cuando realices una **petición de certificado para alguno de tus clientes**, por favor, **proporciona la información de TU COMPAÑÍA (Merkatu)** en nuestra página de petición en el lugar de la del cliente final (recuerda que nosotros contactaremos directamente contigo). No compartas tus códigos de partner con los clientes porque son los códigos propios de tu empresa. **Usar el email webmaster@merkatu.com.**

Incluir el logotipo de miembro del club de partners en tu web. Este logotipo te identificará como distribuidor reconocido de ipsCA y te permitirá beneficiarte de otras características del programa (incluir tu logo en el área de partners de nuestra web, disponer de contenidos de seguridad, etc.) . Puedes encontrar nuestros logos en página web <http://certses.ipsca.com/logos>.

* Una vez hecho esto nos llega un mensaje para realizar el pago a la dirección de email que hemos puesto (webmaster@merkatu.com).

* Una vez hecho el pago nos llegará el mensaje con la factura y, al cabo de un tiempo, el mensaje con el certificado.

Instalación de certificado en RAN

Certificado de godaddy

Dependiendo del tipo de servidor web que usted utilice, necesitará también los archivos nuestro certificado raíz GODADDY, la CA intermedia CA A1 o un archivo combinado de ambas gd-bundle.

Para APACHE añade el certificado de GODADDY (en la casilla certificado CA). La información a adjuntar es [GODADDY certificado raíz](#).

Es **MUY IMPORTANTE** que **INSTALE AMBOS CERTIFICADOS (nuestra CA raíz y la CA intermedia CA A1)** en su servidor web para poder establecer correctamente las sesiones SSL con los navegadores de sus clientes.

Si su servidor es un servidor Microsoft, no requiere instalar la CA Raíz GODADDY, solo la CA Intermedia CA A1.

Si necesita descargar estos certificados de forma individual o en un archivo único, por favor visite nuestra página <http://certs.godaddy.com/>.

Por favor siga las instrucciones específicas de instalación de su servidor localizadas en <http://certs.godaddy.com/>.

Si después de instalar su certificado y comprobando la conexión con un navegador Internet Explorer actualizado usted recibe el error de 'CA no reconocida', esto es debido a que la CA intermedia A1 no se encuentra correctamente instalada

Algunos clientes no instalan o instalan incorrectamente la CA A1 intermedia y reciben errores en sus navegadores 'CA no reconocida' al conectarse a su sitio web.

Certificado de IPSCA

Dependiendo del tipo de servidor web que usted utilice, necesitará también los archivos nuestro certificado raíz IPS SERVIDORES, la CA intermedia CA A1 o un archivo combinado de ambas IPS-IPSCABUNDLE

Es **MUY IMPORTANTE** que **INSTALE AMBOS CERTIFICADOS (nuestra CA raíz y la CA intermedia CA A1)** en su servidor web para poder establecer correctamente las sesiones SSL con los navegadores de sus clientes.

Si su servidor es un servidor Microsoft, no requiere instalar la CA Raíz IPSSERVIDORES, solo la CA Intermedia CA A1.

Si necesita descargar estos certificados de forma individual o en un archivo único, por favor visite nuestra página <http://certs.ipsca.com/support> .

Por favor siga las instrucciones específicas de instalación de su servidor localizadas en <http://certs.ipsca.com/support> .

Si después de instalar su certificado y comprobando la conexión con un navegador Internet Explorer actualizado usted recibe el error de 'CA no reconocida', esto es debido a que la CA intermedia A1 no se encuentra correctamente instalada

Algunos clientes no instalan o instalan incorrectamente la CA A1 intermedia y reciben errores en sus navegadores 'CA no reconocida' al conectarse a su sitio web.

Para comprobar la correcta instalación de su certificado puede utilizar la herramienta que se encuentra en nuestras páginas web <http://certs.ipsca.com/checkserver/> , si esta páginas devuelven una conexión correcta con su servidor, entonces su certificado estará instalado correctamente.

Como parte de nuestro servicio, visitaremos su sitio web, mediante una conexión de navegador, en unos días, para comprobar la instalación correcta del certificado y le remitiremos un informe sobre el funcionamiento de este.

De esta forma nos aseguraremos de la correcta instalación de su certificado.

Pasos siguientes

Entramos como usuario en su panel de control del servidor de RAN para instalar el certificado generado por IPSCA.

Lo hacemos desde Advanced features → SSL Certificates

Elegimos la opción 3 → Paste a pre-generated certificate and key

Aquí añadimos el certificado que nos han mandado en la siguiente línea desde donde termina el CSR que nos han generado a nosotros.

Este certificado es el que se guarda en la web.

The screenshot shows the 'SSL Certificates' management interface. The 'Create your own self signed certificate' option is selected. The 'Common Name' field is populated with 'www.busturialdeaurdaib'. The 'Key Size (bits)' is set to 1024. The 'Paste a pre-generated certificate and key' option is selected, and a large text area contains a private key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAA2jKjQc/Ialvho6xM4u1WoZspbzukUsaBzXhGO6vhWV/pillG
ISf6XpIR7YiVE609ZaEzQzbf6J8KOVfpQYxf9xZnzRrfz+jWkuKGGjiMFP3cPk33e
dHY5faBD6SE1NR4rdvFvDSRY4nTv4KZvbZrk1Dcembd3F00B3FuwcmlkUaku65Kc
QRuHEhnpS1izeyzMCJG7jX2tnUxeOSzNag9EYPm7UaWVGXF2D1DFhmfIpaQ87xMKH
PkWbk1fSDGch0qjBNyXrzDdGvndGrkxIvMfrrmlCB/LQaOw5t421T64UUKFapn5b
Bc0fX/EiyIwJce3TZSIwml9TktfvPbgXJHsWtawIDAQABoIBAQCUCwEbtRTlrg5/
D5C7hSNyud3dv8Ofy0XjVvRK2jugOwt1CkmbKpm+r8cZMeypwYMeLlJO24dcY/+2
DhmP9WNFvPdm9zKWeev6M+UQMj/5rKpNTzrCG3fGdeTWe6UgyY7IYIFdbFJM0XxY
pB+DjY/QPmPWWIYQ1KeYG8qHuJyULoh3IhAWfo6+InBumQiVbciFlhqlzrr19JaJ
j9cZJ8uuAtwdu/pHagmZ+psFGZTweMaCj08faQkj29i+SA+uPaj7QuExaQ4kCET1
kHfC+LK/vhA6v1G8EvLimE1fFC1bP4cqYmEHtP8moT2Q/XkKQZGYQ+QR3800I3tg
KA60q39BAoGBAPSDxtbpt/LnKX268Revmpq/L7wnIx5vaLhVKva337r3g5BYc9Q5
N65mjQQCk+QoIZO/mvImKru08KYym3edRL1hnCeXkWX1o361aze+5TtabpR4YND
mQqm1o6HS9+aRe4jbTNIAPedMxARWPa6zQRFLYMF39xjZGRp9xHRyRD/AoGBANuy
2UvZyRLVn606R7w1GLA9bBJ6pYNIfxiWHxc8JDMaGBaf1WqAHHO7GCRY9uQL45aWG
KTbU7IBHCKc261M/WBRaAAjMGxsRyE/uxDhIqYzW09wXtXbMSFOQz8b+QtwoLAsj
-----
```

Buttons for 'Paste from Clipboard', 'Copy to Clipboard (IE only)', and 'Save' are visible at the bottom of the text area.

Redirigir private_html a public_html

El objetivo de esto es conseguir que tanto las llamadas https como las http se gestionen desde el public_html, con lo que logramos gestionar todo desde el merkagest. Los pasos a seguir son:

1. Entramos como usuario en su panel de control del servidor de RAN 2. Accedemos a Domain setup → clickamos en el nombre de dominio 3. Marcamos esta opción "Use a symbolic link from private_html to public_html - allows for same data in http and https". Nos dirá que se va a eliminar la carpeta private_html junto con su contenido.

The screenshot shows the DirectAdmin interface for managing the domain busturialdeaurdaibai.com. The main configuration area includes fields for Bandwidth (MB) and Disk Space (MB), both set to 0 and checked to be the same as the main account. It also has checkboxes for Secure SSL, CGI Access, and PHP Access, all of which are checked. Below this, the 'private_html' setup section is active, showing two radio button options. The second option, 'Use a symbolic link from private_html to public_html - allows for same data in http and https', is selected. A 'Save' button is visible at the bottom of this section. On the right side, there is a 'Your Account' summary table and a 'Current Domain' section.

Your Account		
Disk Space		
	Used	Max
Disk Space (MB)	14695.0	20000
Bandwidth (GB)	11.915	unlimited
E-Mails	2	unlimited
Rtp Accounts	2	10
Databases	4	5

Current Domain
busturialdeaurdaibai.com

Cambiar la función de googleAnalytics (sólo para urchin)

Esto se aplica sólo para las versiones anteriores a la 2.1.2.1 del merkagest. Es decir, aquellas que accedan al archivo urchin.js

En el archivo **api/api.inc** sustituimos el código actual de la función googleAnalytics por el siguiente:

```
function GoogleAnalytics() {
    if ($this->GetDataTipo()==CONTENIDO_CONTENIDO_DOCUMENTO ||
    $this->googlecode=="") return;
    return ("
        <script type=\"text/javascript\">
            var gaJsHost = ((\"https:\" == document.location.protocol) ?
```

```
\ "https://ssl.\" : \ "http://www.\" );
    document.write(unescape(\ "%3Cscript src='\" + gaJsHost +
\"google-analytics.com/urchin.js'
type='text/javascript'%3E%3C/script%3E\" ));
    </script>
    <script type=\"text/javascript\">
        _uacct = \ ".$this->googlecode.\" \ ";
        urchinTracker();
    </script>
    ");
}
```

Instalación de SSL para un dominio (HOSTALIA)

Muy importante: Guardar en sitio seguro toda la información que usamos para generar los certificados:

Guardar la información en srv-datos/proyectos en curso/<nombre del proyecto>/documentos definitivos/SSL

- CSR que generamos desde el servidor.
- El certificado que nos devuelve IPSCA.

Asignación de IP fija en HOSTALIA

Asignación de una IP fija para el dominio. En este momento tenemos asignadas 5 IP fijas para el servidor.

Nos vamos a 'Ajustes de alojamiento Web' y ahí le ponemos la IP que queremos que tenga (sólo un dominio por cada IP fija). La primera de las fijas **no hay que usarla (82.194.82.253)**.

En caso de que tengamos generado el dominio con anterioridad y ahora le estemos reasignando la IP debemos ir también a Inicio > Direcciones IP > IP que quieras y ahí le reasignas el dominio que quieras.

Generación del certificado SSL

- 1.- Ingresar al panel de plesk y vaya al dominio que quiere que tenga el certificado.
- 2.- Una vez dentro del dominio aprete sobre el icono denominado 'certificados', una vez dentro pulsar 'Añadir certificado'
- 3.- Introduzca El nombre de referencia del certificado y rellene los datos que corresponde al grupo

'preferencias' de manera correcta, luego pulse el boton 'Solicitar'.

4.-Una vez creado, plesk le mostrara el nombre de referencia del certificado. Pulsar sobre el nombre de referencia del certificado para que pueda ver el código CSR y la LLAVE PRIMARIA; antes de estos estan sus datos, los cuales no se pueden editar. Copie ambos en un archivo de texto, incluyendo los titulos que se encuentran entre guiones.

5.-Vaya a su proveedor de certificados e ingrese el CSR que guardo en el anterior paso. El proveedor le dara parte cuando el certificado este listo.

6.-Una vez enviado al proveedor el CSR trate de no borrar el que genero en plesk, por que por más que sean los mismos datos que ingrese el CSR no coincidira con el que tiene(el que envio a su proveedor)

7.-Una vez que tenga el certificado, copielo en un archivo de texto (incluyendo los titulos entre guiones) y guardelo.

8.- Entrar al panel de plesk y vaya al dominio donde creo el certificado. En la opcion 'certificado' (campo examinar) seleccione el archivo donde se encuentra el certificado y luego pulse subir archivo. Si todo marcha bien el certificado se agregara sin problemas.

8.a. - Añada el certificado de GODADDY (en la casilla certificado CA). La información a adjuntar es [GODADDY certificado raiz](#).

8.a. - Añada el certificado de IPSCA (en la casilla certificado CA). La información a adjuntar es [IPSCA certificado CA](#).

9.-Despues de lo anterior ir a configuración del dominio 'Ajustes de alojamiento Web', en donde despues del desplegable de la dirección IP se muestra otro desplegable de los certificados, seleccionar el certificado creado. Luego verificar la casilla 'Soporte SSL'

Cambiar la función de googleAnalytics (sólo para urchin)

Esto se aplica sólo para las versiones anteriores a la 2.1.2.1 del merkagest. Es decir, aquellas que accedan al archivo urchin.js

En el archivo **api/api.inc** sustituimos el código actual de la función googleAnalytics por el siguiente:

```
function GoogleAnalytics() {
    if ($this->GetDataTipo()==CONTENIDO_CONTENIDO_DOCUMENTO ||
    $this->googlecode=="") return;
    return ("
        <script type=\"text/javascript\">
            var gaJsHost = ((\"https:\" == document.location.protocol) ?
    \"https://ssl.\" : \"http://www.\");
            document.write(unescape(\"%3Cscript src='\" + gaJsHost +
    \"google-analytics.com/urchin.js'
    type='text/javascript'%3E%3C/script%3E\");
        </script>
        <script type=\"text/javascript\">
```

```
    _uacct = \".$.this->googlecode.\"";  
    urchinTracker();  
  </script>  
  ");  
}
```

From:

<https://wiki.merkatu.info/> - **Wiki de merkatu**

Permanent link:

https://wiki.merkatu.info/instalar_ssl?rev=1279868291



Last update: **2017/03/27 17:43**