

Moving Toward SSL:

What it is, How to do it, & Why you should care

[Mukalele Rogers, #WordCampKampala](#)

Saturday, 16 December 2017



Hello!

A bit about me...



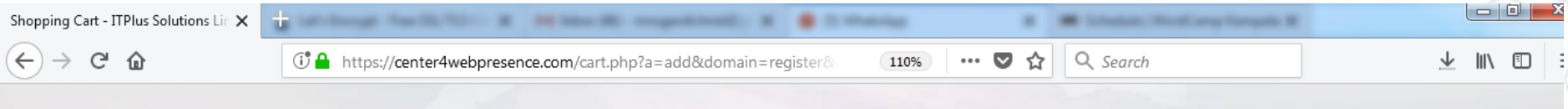
  @mrogers4christ

 www.mukalele.net

What I Do

center4webpresence.com

Offering domain name registration and Web Hosting For Less!
+Free SSL



Categories

- C-Hosting

Actions

- Register a New Domain
- Transfer in a Domain
- View Cart

Choose Currency

UGX

Register Domain

Find your new domain name. Enter your name or keywords below to check availability.

Search bar containing "yrowndomainname" and a "Search" button.

Congratulations! yrowndomainname.com is available!

Shs.45,000/= [Add to Cart](#)


.com <small>HOT</small> Shs.45,000/= Add	.net Shs.48,000/= Add	.org <small>SALE</small> Shs.50,000/= Add	.info Shs.45,000/= Add	.biz Shs.48,500/= Add	.me <small>NEW</small> Shs.47,000/= Add	.work Shs.15,000/= Add	.rocks Shs.25,000/= Add
--	---	---	--	---	---	--	---

What I Do

As an ICT Teacher / Trainer, I maintain an online shop powered by  +  **WooCommerce** at mukalele.net

Mukalele Rogers | Official Website

ICT Specialist, Web Programmer, Lover of God's Word

SIGN IN / REGISTER | 1 ITEM - SHS.35,000 CHECKOUT 

HOME

ABOUT ME

PRODUCTS AND SERVICES

UPDATES

SHOP


CONTACTS


GO TO SHAREBILITY

HOME / SHOP

Shop

Showing all 5 results

DEFAULT SORTING 

Search... 

RECENT POSTS

INFORMATION ON 56 LEAVERS
PUJAB FORMS FOR 2017/2018
ACADEMIC YEAR

See you at WordCamp Kampala 2017
as we discuss Web Development
with WordPress

UNEB releases Subsidiary ICT
Support Files 2017, grants public
download

Walking by Faith, Not by Sight
Love for God's Word

SOME EVENTS TO ATTEND

WORDCAMP KAMPALA
2017

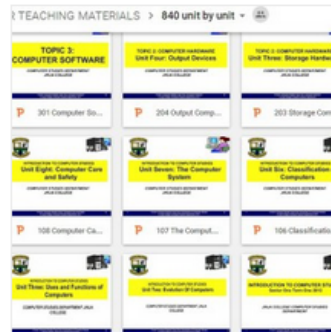
December 16 @ 8:30 am -
December 17 @ 6:45 pm



COMPUTER STUDIES for
Uganda – Fifth Edition 2017

Shs.35,000

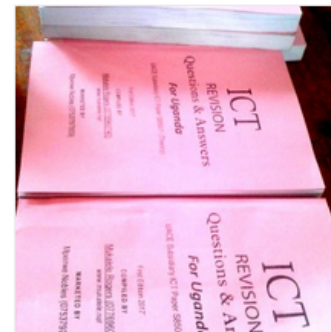
Add to cart



Computer Studies Teaching
PowerPoint, PDF Notes

Shs.500

Add to cart



ICT Revision Questions and
Answers for Uganda Booklet
1st Edition 2017

Shs.10,000

Add to cart

What I Do

Sharebility Uganda - sharebility.mukalele.net

An educational digital resource sharing system for Ugandan Schools

The screenshot shows the Sharebility Uganda website interface. On the left is a dark sidebar with the Sharebility logo and navigation links: Home, About, Register, Upload, Usage by District, RESOURCE CATEGORIES, Primary, P1, P2, P3, P4, P5, P6, P7, Secondary, and S1. The main content area features a 'Home' button, a search bar with a magnifying glass icon and a 'Go!' button, and a 'Featured Resources' section. The featured resources include:

- King's College, Budo Uganda Advanced Certificate Of Education Mock 1 Examination 2015 Applied Mathematics Paper 2 (1704 DOWNLOADS)
- **New** Support Files Compilation For Sub Ict Past Paper Exams And Lab Activities Book Questions (1690 DOWNLOADS)
- Uneb Uce Computer Studies Paper One 2009 Examination Past Paper (1438 DOWNLOADS)
- Book Preview: Lab Activities For Computer Practical Applications Covers Uace S850/2 And Uce 840/2 (1373 DOWNLOADS)



Moving Toward SSL

Posted December 1, 2016 by [Matt Mullenweg](#). Filed under [Development](#).

We're at a turning point: 2017 is going to be the year that we're going to see features in WordPress which require hosts to have HTTPS available. Just as JavaScript is a near necessity for smoother user experiences and more modern PHP versions are critical for performance, SSL just makes sense as the next hurdle our users are going to face.

SSL basically means the link between your browser and the server is encrypted. SSL used to be difficult to implement, and often expensive or slow. Modern browsers, and the incredible success of projects like [Let's Encrypt](#) have made getting a certificate to secure your site fast, free, and something we think every host should support by default, especially in a post-Snowden era. Google also weighs [SSL as a search engine ranking factor](#) and will begin [flagging unencrypted sites in Chrome](#).

First, early in 2017, we will only promote hosting partners that provide a SSL certificate by default in their accounts. Later we will begin to assess which features, such as API authentication, would benefit the most from SSL and make them only enabled when SSL is there.

Separately, I also think the performance improvements in PHP7 are particularly impressive, and major kudos to everyone who worked on that. We will consider whether hosts use PHP7 by default for new accounts next year as well.

See Also:

For more WordPress news, check out the [WordPress Planet](#).

There's also a development P2 blog.

To see how active the project is check out our [Trac timeline](#), it often has 20-30 updates per day.

Categories

- [Releases](#) (206)
- [Development](#) (191)
- [Security](#) (47)
- [Community](#) (43)
- [Meta](#) (43)
- [Events](#) (33)
- [Testing](#) (23)
- [WordCamp](#) (20)
- [General](#) (18)
- [Documentation](#) (15)

A decorative network diagram in the top-left corner, consisting of various sized nodes (some solid, some hollow) connected by thin lines, forming a complex web structure.

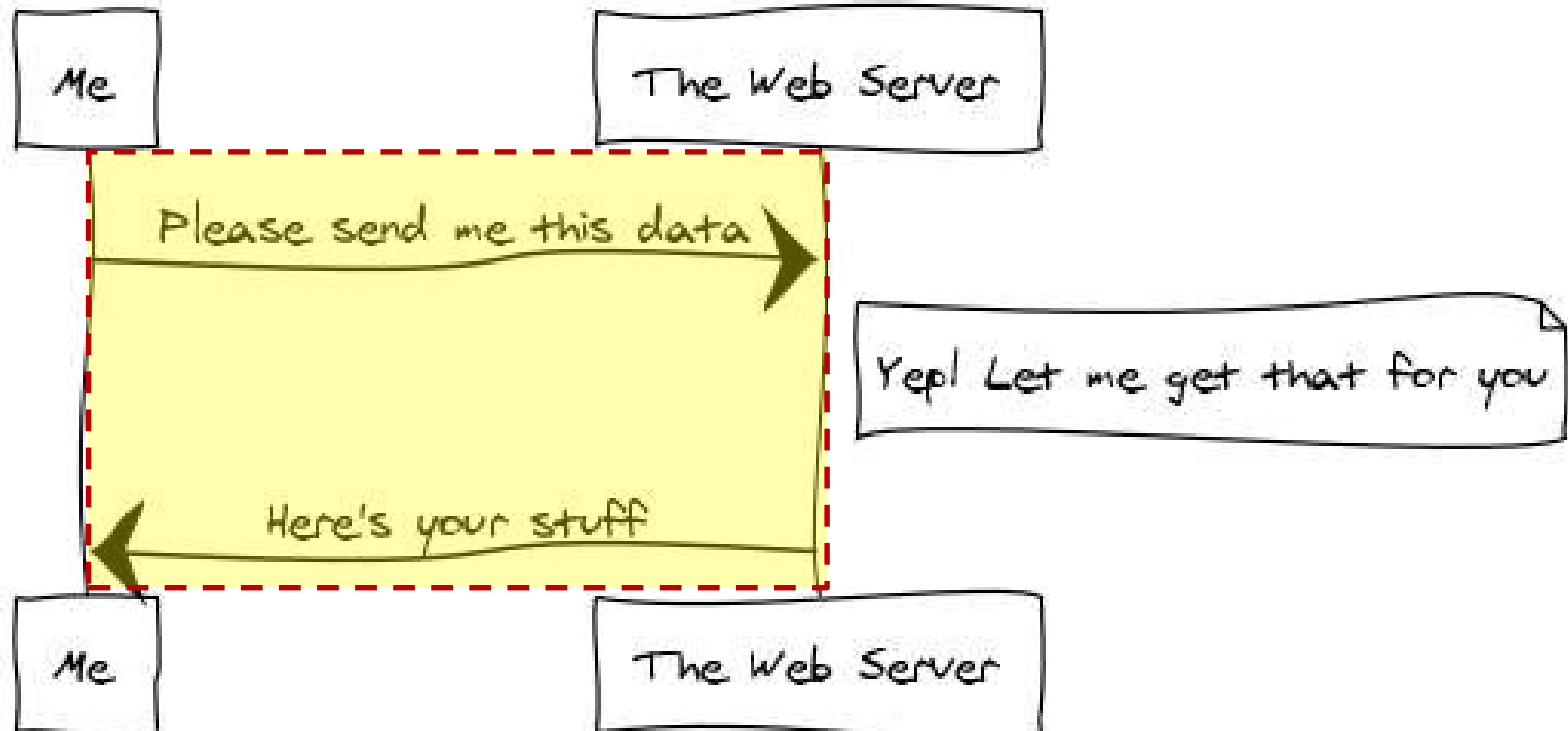
1.

SSL: What it is

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, with nodes and connecting lines.

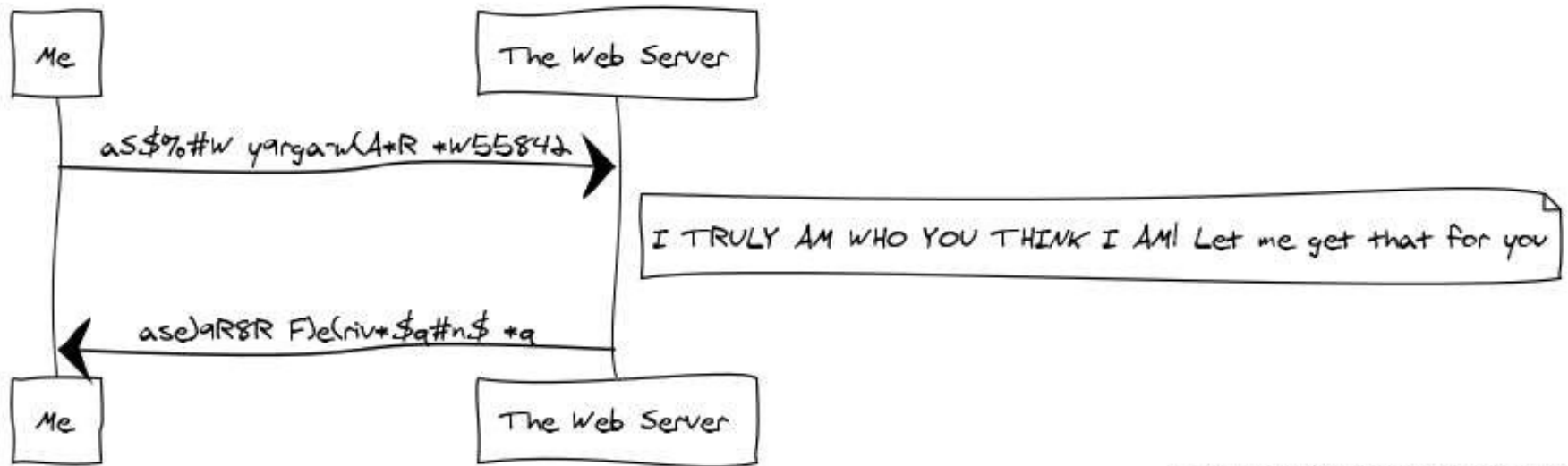
HTTP Review

The HTTP



HTTPS

The HTTPS



HTTP vs HTTPS

sends password



helloworld

HTTP

Receives password



Hacker hacks the link
and gets your password
"helloworld"

sends password



helloworld

ENCRYPTED

HTTPS

"Xu587Tyus)"

Receives password



helloworld

DECRYPTED

HACKER

Hacker hacks the link
and gets password as
"Xu587Tyus)"

How does HTTPS work: SSL explained

This presumes that SSL has already been issued by SSL issuing authority.



A decorative network diagram consisting of interconnected nodes and lines, rendered in a light gray color. The nodes are represented by small circles, some of which are larger and have a double-circle outline. The lines connect these nodes in a complex, web-like structure. This graphic is positioned in the top-left and bottom-right corners of the slide.

2.

Why you should care

Who Needs It?

- ◎ E-Commerce
- ◎ Social Media
- ◎ Form Data e.g wp-login form
- ◎ Mandatory for many functionalities **See goo.gl/LoY7u5**
e.g. Geolocation, Device motion, EME, getUserMedia, AppCache, Notifications
- ◎ SEO for websites
- ◎ Everyone!



Username or Email Address

Password

Remember Me

Log In

[Lost your password?](#)

[← Back to bitworx](#)

Google +  SSL = 

Eventual treatment of all
HTTP pages in Chrome:

 Not secure | example.com

A decorative network diagram in the top-left corner, consisting of various sized grey circles connected by thin grey lines, forming a complex web-like structure.

3.

How to do it

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, with grey circles of different sizes connected by thin grey lines.

You'll Need...

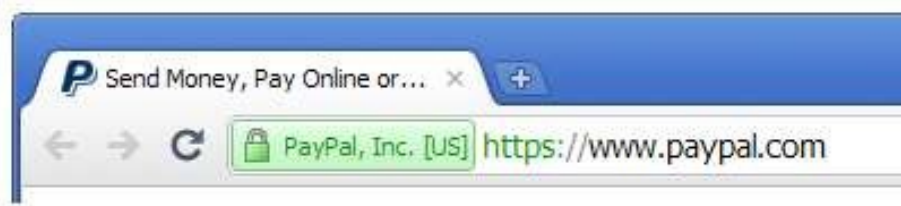
```
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIQKAIzIUrmTHxcwwABHyda7ZANBgkqhkiG9w0BAQUFADBZ
MQswCQYDVQQGEWJHQjEbmBkGA1UECBMSR3JlYXRlcjBNYw5jaGVzdGvYMRAdGyD
VQQHEwdTYWxmb3JkMRowGAYDVQQKEXFDT01PRE8gQ0EgTGltaxRlZDEZMBCGA1UE
AxMQUG9zaXRpdmVTU0wGQ0EgMjAeFw0xNDAzMDUwMDAwMDBaFw0xNTAzMDUyMzU5
NTl1amF0eXITAFBGNVBASTGERvbWVpbWVDb250cm9sIFZhbG1kYXRlZDEUMBIGA1UE
CxMLUG9zaXRpdmVTU0wXHZAdBgNVBAMTFnd3dy5qb2hudG90agV3b3JzSz5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCs75Fnemzt a920HfVIPq1
+5kbfzudowwGyEFdsfhBY9Y4LM0P0j2+tKPiuzy1qgKE9g43jef+6PXmqlCXUJ6S
HNwz0TDDgUuEmjTGGzdjd+vuu0io3DkuqRn3a6VUmr mquKlYlZQK1Bzec+fGxbI7
BTfws3w1TLPenGRAUZGjxj4Cwnf6XAnuXsr7beHGltaefov1qz4JPzdd78QXRiWQ
08lNDDR eiJHPQaabWIELF0fm/a4+kwm4GwFAd6SDMCAG5ChpswwqLMzrujfcMDRV
vNTau8UNAorUYfosShbeyf5F/EER/9NKh2Y1rKJF7TsY9GjzD/MSOX5H1Tx0Zdn1
AgMBAAAGjggG1MIIBSTAFBGNVHSMEGDAwGBSZ5EBfaxRePgXZ3dnjVPxiuPCAR DAD
BGNVHQ4EFgqu19iRosAURI7hur0c8abfwwubr5MwdgYDVR0PAQH/BAQDAgwgMAwG
A1UdeWEB/wQCMAAWHQYDVR01BBYWFAYIKwYBBQUHAWEGCCsGAQUFBwMCMFAGA1Ud
IARJMEcwowYLKwYBBAGyMQEACgWLDaQBggrBgEFBQCCARYeahR0cdovL3d3dy5w
b3NpdG12ZXNzbc5jb20vQ1BtMAGBmeBDAECATA7BgnVHR8ENDAYMDCgLaShi po
dHRwoi8vY3JzLmNvbW9kb2NhlMnVbs9Qb3NpdG12ZVNTTENBmi5jc mwwbAYIKwYB
BQUHAQEYDBEMDYGCCsGAQUFBzAchi podHRwoi8vY3J0LmNvbW9kb2NhlMnVbs9Q
b3NpdG12ZVNTTENBmi5jc nQwJAYIKwYBBQUHMAGGGH0dHA6Ly9vY3NwLmNvbW9k
b2NhlMnVbTA1BgNVHREELjAsghz3d3cuam9obnrVdgh1d29ybGQuY29tghJqb2hu
dG90agV3b3JzSz5jb20wDQYJKoZIhvcNAQEFBQADggEBAJgjwJvrIcOEYF110Eko
qwVqb5ZB7f61Zk0dhcUVE4Jo7uSE5K2i38D9bjSntmt6jzVrNJwr1NRE4YPZvwHE
b9T8XKSyk8iU4qfk+Bdve/DZVZygluo419i487vti2/7Gp/kIPpUFG+xqxh/oQM7
B90xvhbnx/nei uht4tFKB89t1vEX7cq22291/vvs/BXWJfcuc5RZ1LB9qmKdzMpy
oo+a056tk0gjja/2XhLANzBTEmof8p10jJxm3awp1x0ZHV+1fpcaxCBKWB35M9mc
np7EZMq1gdaTutqRIvGxxAe8MvVOESbmZZ5mqA5AYrUH12APDz6GxQM9FHPS17wx
8QA=
-----END CERTIFICATE-----
```

Certificate contents

- ◎ Domain name (common name)
- ◎ Public key
- ◎ Owner of certificate (subject)
- ◎ Issuer of certificate (CA)
- ◎ Expiration data
- ◎ Serial number

Types of Certificates

- ⦿ Domain Validation – CA checks right of applicant to use domain name
- ⦿ Organization Validation – CA does above + vets organization
- ⦿ Extended Validation – CA does above + thorough vetting of organization



Basic Steps for Adding SSL

1. Generate a CSR (certificate signing request) at your web host
2. Buy a certificate from a vendor
3. Validate your domain/certificate
4. Send the CSR, certificate, and bundle files to your web host
5. Configure your site to use SSL
6. Upon renewal, repeat steps #1-4

RAPIDSSL CERTIFICATE

Starting at

\$49.95

USD annually

👍 Dynamic VPS, Cloud & Flex Servers

- ✓ **Secure** Site Seal
- ✓ **256** Bit Encryption

GET RAPIDSSL

GLOBALSIGN ONECLICK ALPHA

MOST POPULAR!

Starting at

\$49.95

USD annually

👍 Web Hosting, Managed VPS & Managed Dedicated

- ✓ **Secure** Site Seal
- ✓ **256** Bit Encryption
- ✓ **1-Click** Setup
- ✓ **Requires** cPanel

GET ALPHA

GLOBALSIGN ONECLICK DOMAIN VERIFIED

Starting at

\$129.95

USD annually

👍 For our cPanel managed accounts

- ✓ **Verified** Domain
- ✓ **256** Bit Encryption
- ✓ **1-Click** Setup
- ✓ **Requires** cPanel

GET GLOBALSIGN

SSL Certificate Solutions

GLOBALSIGN ALPHA WILDCARD

Starting at

\$149.95

USD annually

- ✓ **Secure** Site Seal
- ✓ **Unlimited** Subdomains
- ✓ **256** Bit Encryption
- ✓ **2048** Bit Key

[GET ALPHA](#)

GLOBALSIGN DOMAIN VERIFIED WILDCARD

MOST POPULAR!

Starting at

\$449.95

USD annually

- ✓ **Secure** Site Seal
- ✓ **Unlimited** Subdomains
- ✓ **256** Bit Encryption
- ✓ **2048** Bit Key
- ✓ **Domain** Authentication

[GET GLOBALSIGN](#)

GLOBALSIGN ORGANIZATION VERIFIED WILDCARD

Starting at

\$499.95

USD annually

- ✓ **Secure** Site Seal
- ✓ **Unlimited** Subdomains
- ✓ **256** Bit Encryption
- ✓ **2048** Bit Key
- ✓ **Organization** Authentication

[GET GLOBALSIGN](#)



Let's Encrypt

- Free, automated, open Certificate Authority
- Domain validation
- 3-month expiry

MAJOR SPONSORS



letsencrypt.org

Lets Encrypt Support

Providers that Enable Let's Encrypt and Redirect HTTP->HTTPS by Default

This is the best support of Let's Encrypt's mission "to create a more secure and privacy-respecting Web."

- [EasyStore.co](#) 4.2k (Source 324)
- [Inspedium Corp.](#) 270 (Source 20)
- [manitu](#) 1.8k (Source 81)
- [Neocities](#) 2.5k (Source 137)
- [Netsite](#) 369 (Source 13) (both in Danish)
- [Pride Tech Design](#) 174 (Source)
- [Shopify](#) 397 (Source 97)
- [Squarespace](#) 2.5k (Source 254)
- [Tumblr](#) 130 (Source 32)
- [WordPress.com](#) 7.8k (Source 2.7k)
- [XS4ALL](#) 2.2k (Source)

Web Hosting Providers with Let's Encrypt Support

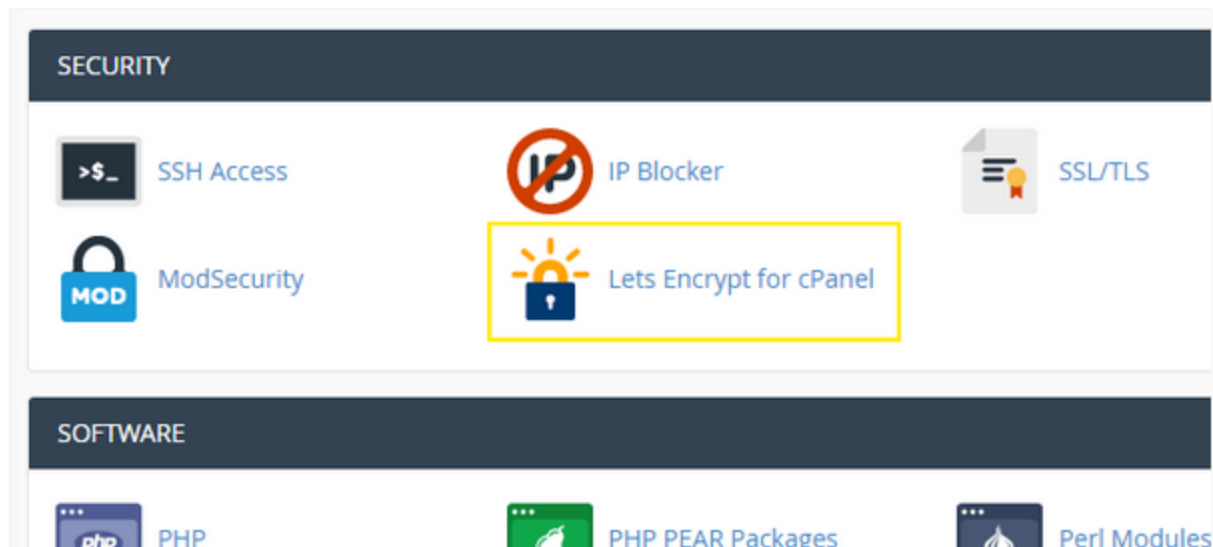
- [1and1.co.uk](#) 691 (Source)
- [34SP.com](#) 2.0k (Source 311)
- [a2hosting.com](#) 4.4k (Source 1.7k)
- [Active24.co.uk](#) 1.1k (Source 84)
- [Active24.cz](#) 624 (Source 144)
- [all-inkl.com](#) 1.8k (Source 629, more detailed instructions 1.7k) (both in German)
- [Antagonist](#) 446 (Source 67)
- [Antilope Hosting](#) 144 (Source 4)
- [Apis Networks](#) 628 (Source 57)
- [blueboard.cz](#) 552 (Source 39)

Full List goo.gl/1BsdZF

Lets Encrypt plugin for cPanel

Installing a Certificate

Once you're logged into cPanel, you should see a **Let's Encrypt for cPanel** button under **Security**. Click on it to access your active domains list to install a certificate.



All the issued certificates are *Cross-signed* by **IdenTrust**. In this way, all the L.E. certificates are trusted by major browsers.

Details: goo.gl/uHF8rS

Tool for Generating Certificates in Minutes



SSL For Free

Free SSL Certificates in Minutes

 <https://>enter your website to secure

Create Free SSL Certificate

[Advanced Options](#)



100% Free Forever

Never pay for SSL again. Thanks to [Letsencrypt](#) the first non-profit CA.



Widely Trusted

Our free SSL certificates are trusted in 99.9% of all major browsers.



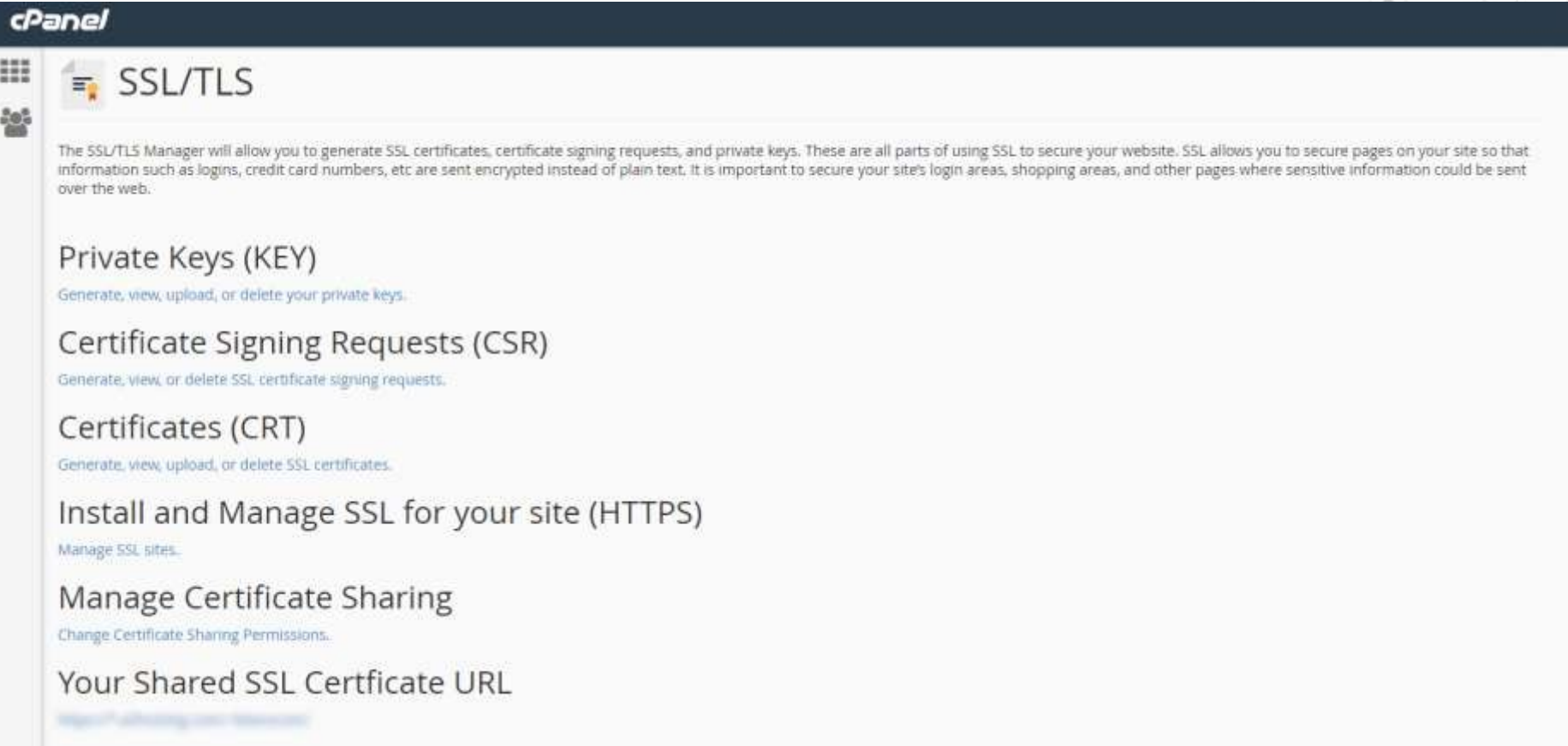
Enjoy SSL Benefits

- Protect user data & gain trust
- Improve Search Engine Ranking
- Prevent forms of website hacking

Wildcard Certificates Supported? They are not supported but you can add up to 100 domains and or subdomains per certificate.

Details: sslforfree.com

cPanel SSL/TLS Manager

The image shows a screenshot of the cPanel SSL/TLS Manager interface. At the top left is the cPanel logo. Below it is a navigation menu with icons for a grid, a lightbulb, and a group of people. The main heading is "SSL/TLS" with a lightbulb icon. A descriptive paragraph explains the purpose of the manager. Below this are several menu items, each with a sub-description: "Private Keys (KEY)", "Certificate Signing Requests (CSR)", "Certificates (CRT)", "Install and Manage SSL for your site (HTTPS)", "Manage Certificate Sharing", and "Your Shared SSL Certificate URL".

cPanel

SSL/TLS

The SSL/TLS Manager will allow you to generate SSL certificates, certificate signing requests, and private keys. These are all parts of using SSL to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card numbers, etc are sent encrypted instead of plain text. It is important to secure your site's login areas, shopping areas, and other pages where sensitive information could be sent over the web.

Private Keys (KEY)

Generate, view, upload, or delete your private keys.

Certificate Signing Requests (CSR)

Generate, view, or delete SSL certificate signing requests.

Certificates (CRT)

Generate, view, upload, or delete SSL certificates.

Install and Manage SSL for your site (HTTPS)

Manage SSL sites.

Manage Certificate Sharing

Change Certificate Sharing Permissions.

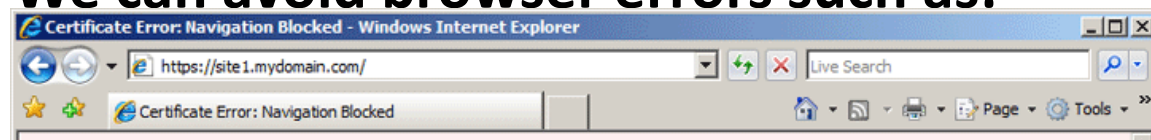
Your Shared SSL Certificate URL

[View Shared SSL Certificate URL](#)

Validity

- Lets Encrypt certificates have a **90 days** validity. After the expiry, the certificates are not valid anymore and the browsers will raise security errors.
- You will receive *remind emails* whenever a certificate is near to expire. Certificate renewal can be automated with a **cron** task.

We can avoid browser errors such as:



A security warning dialog box from Internet Explorer. It features a red shield icon with a white 'X'. The text reads: 'There is a problem with this... The security certificate presented by... Security certificate problems may inc... server. We recommend that you close th... Click here to dose this webpage. Continue to this website (not rec... More information'. At the bottom, there is a 'Done' button and a link to 'SSL Shopper.com'.

A Chromium browser error page titled 'Secure Connection Failed'. It features a yellow warning icon. The text says: 'cogito.ferrus.net uses an invalid se... The certificate is not trusted becaus... (Error code: sec_error_untrusted_is...'. Below this, there are two bullet points: 'This could be a problem with the serv... someone trying to impersonate the s...' and 'If you have connected to this server s... may be temporary, and you can try a...'. At the bottom, there is a link: 'Or you can add an exception...'. The background is a light gray with a subtle grid pattern.

An 'SSL Error - Chromium' dialog box. It has a dark gray header. The main content area has a white background with a red border. It features a yellow warning triangle icon. The text reads: 'The site's security certificate is not trusted! You attempted to reach... but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chromium cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.' At the bottom, there are two buttons: 'Proceed anyway' and 'Back to safety'. A link 'Help me understand' is at the very bottom.



WordPress SSL / HTTPS Tools

- ◎ Update Site URL from http:// to https://
- ◎ Force http requests to https

Add Plugins [Upload Plugin](#)

[Search Results](#) [Featured](#) [Popular](#) [Recommended](#) [Favorites](#)



Really Simple SSL


No setup required! You only need an SSL certificate, and this plugin will do the rest.

By Rogier Lankhorst

[Install Now](#) [More Details](#)

★★★★★ (21)
3,000+ Active Installs

Last Updated: 1 month ago

✓ Compatible with your version of WordPress 



Why No Padlock?

Here's a simple tool that will tell you about any insecure items on your SSL page!



Why No Padlock?

[Home](#) | [FAQ](#) | [About](#) | [Contact](#)

Domain Name: www.lexicoonn.com
URL Tested: <https://www.lexicoonn.com/makepayment.html>
Number of items downloaded on page: 29

Valid Certificate found.

Certificate valid through: Dec 12 17:47:24 2011 GMT
Certificate Issuer: GeoTrust Inc

Total number of items: 103
Number of insecure items: 7

Insecure URL: <http://fonts.googleapis.com/css?family=Lato:100,400,700>
Found in: <https://wordpress.com/>

Insecure URL: <http://en.blog.files.wordpress.com/2011/05/vertigo-blog>
Found in: <https://wordpress.com/>

Insecure URL: <http://theme.files.wordpress.com/2011/11/adventure-jou>
Found in: <https://wordpress.com/>

1. Extended Validation SSL - Green Bar

PayPal, Inc. [US] <https://www.paypal.com>

2. Standard Validation SSL - No Bar

<https://moz.com/checkout/freetrial>

3. SSL with Errors

<https://www.dunkindonuts.com/dunki...>



Removing SSL

© wp-config.php

© .htaccess

© Updating site URL (functions.php)

```

13 *
14 * @package WordPress
15 */
16
17 // ** MySQL settings - You can get this info from your web host ** //
18 /** The name of the database for WordPress */
19 define( 'DB_NAME', 'economicblogs_db' );
20
21 /** MySQL database username */
22 define( 'DB_USER', 'economicblogs_db' );
23
24 /** MySQL database password */
25 define( 'DB_PASSWORD', '2dC29qArwq' );
26
27 /** MySQL hostname */
28 define( 'DB_HOST', 'localhost' );
29
30 /** Database Charset to use in creating database tables. */
31 define( 'DB_CHARSET', 'utf8mb4' );
32
33 /** The Database Collate type. Don't change this if in doubt. */
34 define( 'DB_COLLATE', '' );
35
36 define('FORCE_SSL_ADMIN', true);
37
38 /**#@+
39 * Authentication Unique Keys and Salts.
40 *
41 * Change these to different unique phrases!
42 * You can generate these using the (link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service)
43 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
44 *
45 * @since 2.6.0

```

Currently editing: /home2/bonzrco/public_html/.htaccess

```

RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

```



A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow with a light blue outline. The connections form a complex, branching structure.

Thanks!

Demo Time and questions.

A decorative network diagram in the bottom left corner, similar to the one in the top right, featuring nodes of different sizes and colors (solid grey and hollow light blue) connected by thin lines.