



**300 Seconds of Fame:  
November 2015**



**Let's Encrypt**

Drew Fustini  
@pdp7

# Let's Encrypt is a new Certificate Authority: **It's free, automated, and open.**

In Limited Beta

## FROM OUR BLOG

Nov 9, 2015

### [Why ninety-day lifetimes for certificates?](#)

We're sometimes asked why we only offer certificates with ninety-day lifetimes. People asking this are usually concerned that this is too short and wish we would offer certificates lasting a year or more, like some other CAs do.

[Read more](#)

## MAJOR SPONSORS

mozilla



**IdenTrust**  
part of HID Global





# Let's Encrypt

## New Certificate Authority:

- Free
- Automated
- Open



# Let's Encrypt

- As of October 2015, certificates are now:

**Trusted by all major browsers**

- **Beta Participation Request**



https://helloworld.letsencrypt.org

helloworld.letsencrypt.org

Your connection to this site is private.

Permissions

Connection



The identity of this website has been verified by Let's Encrypt Authority X1. No Certificate Transparency information was supplied by the server.

[Certificate information](#)



Your connection to helloworld.letsencrypt.org is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES\_128\_GCM and uses ECDHE\_RSA as the key exchange mechanism.

[What do these mean?](#)



# Hello World, Let's Encrypt.

Let's Encrypt is a new certificate authority. We created this page to show you our first certificate.

## WE'RE TRUSTED

Let's Encrypt is now trusted by a majority of the web browsers, as planned in our [launch schedule](#). Website users no longer need to add our [ISRG root certificate](#) to utilize certificates issued by Let's Encrypt.

Now that we're trusted, this page should have loaded without errors or warnings, and you should see a lock icon in the URL bar. Click the lock! In the security information, you should see something like "Verified by: Let's Encrypt". You can use your browser's certificate viewer to see the details of the certificate.

## GET INVOLVED

Let's Encrypt is a community-driven project. We would love for you to get involved.

- Help us build the [CA](#) and [client](#)
- Participate in the [community support forums](#)
- Apply to get a certificate as part of our [beta program](#)
- Sign up to be a [sponsor](#)



# Let's Encrypt

## Internet Security Research Group

- Federal 501(c)(3) Non-Profit
- Mission: **reduce** financial, technological, and education **barriers** to **secure communication** over the **Internet**
- *Board members from*: EFF, Stanford Law, CoreOS, Akamai, Cisco, University of Michigan

Platinum

mozilla



Gold



Silver

AUTOMATTIC





# Let's Encrypt

- **Client Software:**

Let's Encrypt is a **Python**-based utility that works alongside **Apache** to automatically obtain a certificate and convert a website to HTTPS.

- **Server-side CA Software:**

**Boulder** is the primary Let's Encrypt CA implementation. It's based on the **ACME** protocol, and written primarily in **Go**.





# Let's Encrypt

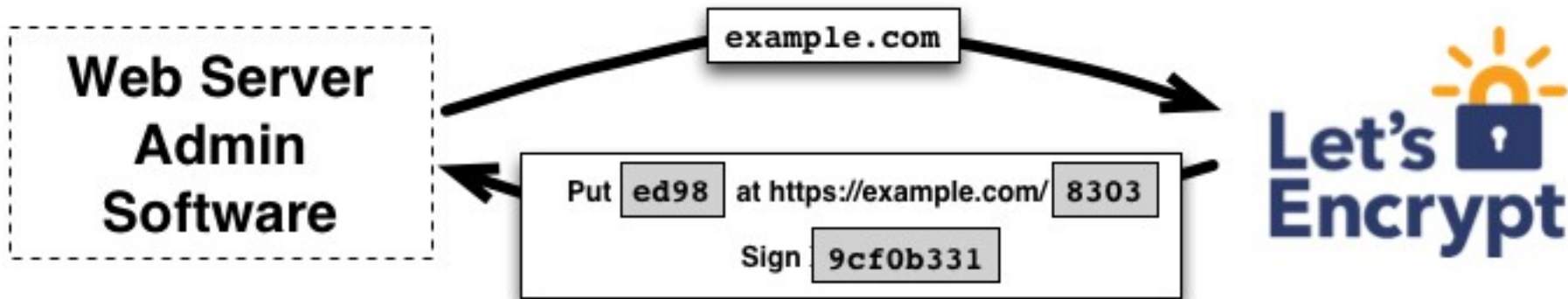
## ACME Protocol

- Let's Encrypt CA talks to certificate management software running on web servers
- Protocol for this is called **ACME**:  
**Automated Certificate Management Environment**
- **Draft Specification**
  - Will be proposed to IETF to make it open standard



# Let's Encrypt

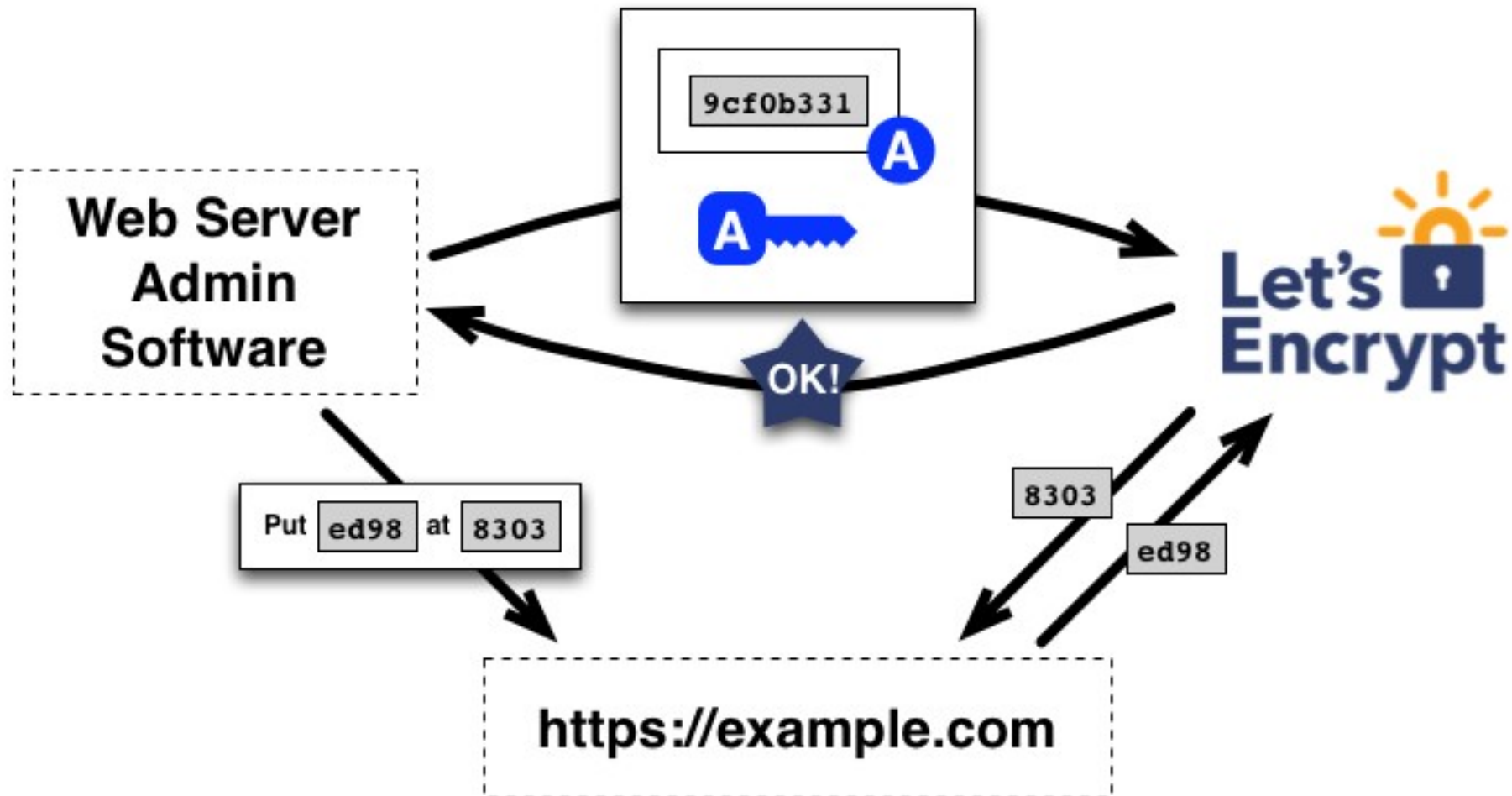
## Domain Validation





# Let's Encrypt

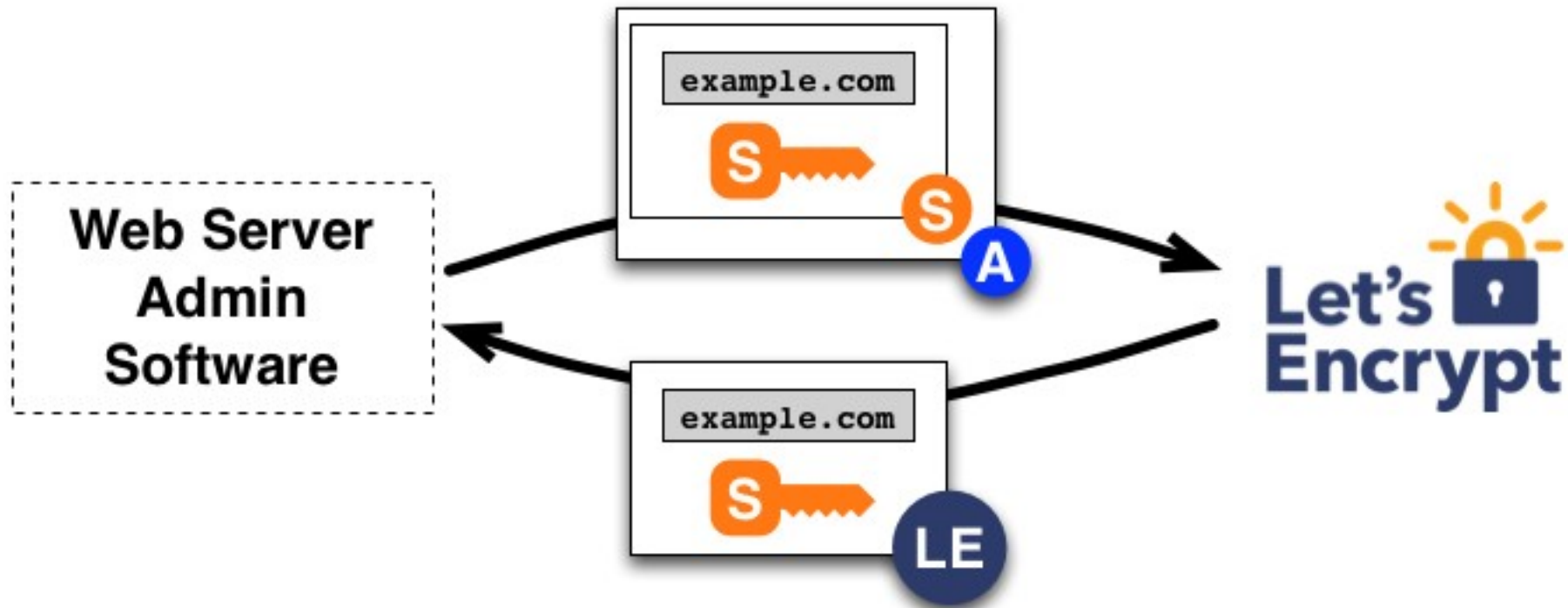
## Domain Validation





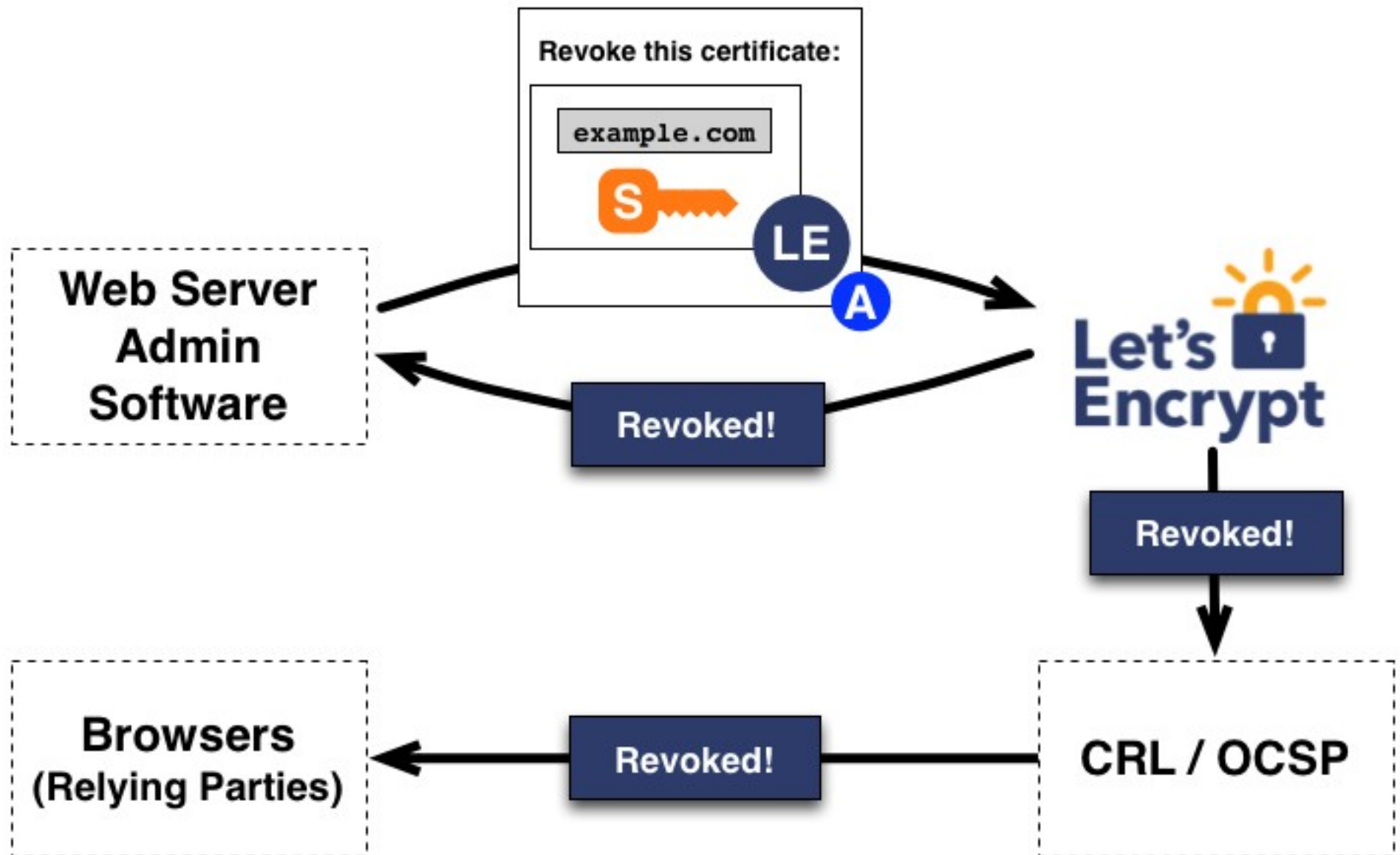
# Let's Encrypt

## Certificate Issuance and Revocation





# Let's Encrypt



# Let's Encrypt Beta Participation Request

Please fill out this form to request participation in the Let's Encrypt beta program.

If you are selected for participation we will email you when we are ready for you to request certificates for your domains. Note that if selected you will still have to perform domain validation. Unfortunately we cannot guarantee that we'll be able to accommodate your request.

For questions about how to request or manage Let's Encrypt certificates, please visit:

<https://community.letsencrypt.org/>

**\* Required**

**What domain(s) would you like to get a certificate for? \***

Separate multiple domains with a comma.

pdp7.com

**What email address can we contact you at when we're ready for you? \***

Your email address will be kept confidential and deleted when the beta program ends.

drew@pdp7.com

**Submit**

*Never submit passwords through Google Forms.*

# Let's Encrypt Closed Beta Invite

2 messages

Let's Encrypt Beta <betaprogram@letsencrypt.org>  
To: drew@pdp7.com

Tue, Nov 3, 2015 at 6:47 PM

Greetings from Let's Encrypt, [drew@pdp7.com](mailto:drew@pdp7.com).

Thank you for your interest in our beta program! We're excited to let you know that your domains (below) have been whitelisted, and you can now utilize an ACME client to obtain a certificate for them.

## Quick Start

To use Let's Encrypt's official client to obtain your real certificates, you will need to provide the production API URL on the command line:

<https://acme-v01.api.letsencrypt.org/directory>

When running the Python client (installation directions [1]), be sure to specify the `--server` argument with the production URL:

```
git clone https://github.com/letsencrypt/letsencrypt
cd letsencrypt
./letsencrypt-auto --agree-dev-preview --server \
https://acme-v01.api.letsencrypt.org/directory auth
```

If you are using a different ACME client, be sure to configure it to use the production URL in order to get valid certificates. Many clients will default to the staging URL.

How would you like to authenticate with the Let's Encrypt CA?

- 1 Apache Web Server - Alpha (apache)
- 2 Automatically use a temporary webserver (standalone)

< OK >

< Cancel >

<More Info>



Please read the Terms of Service at  
<https://letsencrypt.org/documents/LE-SA-v1.0.1-July-27-2015.pdf>. You  
must agree in order to register with the ACME server at  
<https://acme-v01.api.letsencrypt.org/directory>

<Agree >

<Cancel>

Please enter in your domain name(s) (comma and/or space separated)

pdp7.com

< OK >

<Cancel>



# Let's Encrypt

- Your certificate and chain have been saved at:

**`/etc/letsencrypt/live/pdp7.com/fullchain.pem`**

- Your cert will expire on:

**`2016-02-07`**

- To obtain a new version of the certificate in the future, simply run Let's Encrypt again.
- Your account credentials have been saved in your Let's Encrypt configuration directory at:

**`/etc/letsencrypt`**

- You should make a secure backup of this folder now. This configuration directory will also contain certificates and private keys obtained by Let's Encrypt so making regular backups of this folder is ideal.

- My **pdp7.com** hosted by **Debian 8.2** server on **DigitalOcean**
- **Apache SSL Config file:**

**/etc/apache2/sites-enabled/default-ssl.conf**

```
<IfModule mod_ssl.c>
    <VirtualHost *:443>
        SSLEngine on
        SSLProtocol               all -SSLv2 -SSLv3
        SSLCipherSuite             ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128
        SSLHonorCipherOrder        on
        SSLCompression             off
        SSLCertificateFile /etc/letsencrypt/live/pdp7.com/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/pdp7.com/privkey.pem
        ServerSignature Off
        AcceptPathInfo Off
        AddOutputFilterByType DEFLATE text/html text/plain text/xml applicati
        AddDefaultCharset UTF-8
        SSLOptions +StrictRequire
        ServerAdmin admin@pdp7.com
        ServerName pdp7.com
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i
            LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common
    </VirtualHost>
</IfModule>
```

gpg key: [pdp7.pub.asc](#)

fingerprint = D869 9E3B 6AB1 63C0 AE99 FD71 84D4 4A93 17F1 138E

[Join EFF!](#)**ELECTRONIC FRONTIER FOUNDATION**

The [Electronic Frontier Foundation](#) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, [EFF](#) champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

Even in the fledgling days of the Internet, [EFF](#) understood that protecting access to developing technology was central to advancing freedom for all. In the years that followed, [EFF](#)



General



Media



Permissions



Security

### Website Identity

Website: **pdp7.com**Owner: **This website does not supply ownership information.**Verified by: **Let's Encrypt**[View Certificate](#)

### Privacy & History

Have I visited this website prior to today? **Yes, 76 times**Is this website storing information (cookies) on my computer? **No**[View Cookies](#)Have I saved any passwords for this website? **No**[View Saved Passwords](#)

### Technical Details

**Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bit keys, TLS 1.2)**

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

General

Details

This certificate has been verified for the following uses:

SSL Server Certificate

**Issued To**

Common Name (CN) pdp7.com  
Organization (O) <Not Part Of Certificate>  
Organizational Unit (OU) <Not Part Of Certificate>  
Serial Number 01:BE:53:8B:4F:98:12:88:04:46:47:E2:54:00:28:FB:46:B0

**Issued By**

Common Name (CN) Let's Encrypt Authority X1  
Organization (O) Let's Encrypt  
Organizational Unit (OU) <Not Part Of Certificate>

**Period of Validity**

Begins On 11/08/2015  
Expires On 02/06/2016

**Fingerprints**

SHA-256 Fingerprint D1:98:26:91:19:35:0D:9F:C1:78:D8:AF:F1:32:60:B9:  
E7:9E:A8:6F:9A:E2:FE:31:27:9E:DD:F3:BA:66:32:F2  
SHA1 Fingerprint 19:3F:83:8C:00:B3:04:5B:ED:45:3B:6A:99:00:37:AA:C7:D8:CD:E6

Close

General Details

**Certificate Hierarchy**

[-] DST Root CA X3

[-] Let's Encrypt Authority X1

pdp7.com

**Certificate Fields**

[-] Validity

Not Before

Not After

[-] Subject

[-] Subject Public Key Info

Subject Public Key Algorithm

Subject's Public Key

[-] Extensions

Certificate Basic Constraints

Certificate Key Usage

Certificate Subject Key ID

**Field Value**

CN = DST Root CA X3

O = Digital Signature Trust Co.

Export...


Close



**pdp7.com** x

Your connection to this site is private.

Permissions **Connection**

 The identity of this website has been verified by Let's Encrypt Authority X1. No Certificate Transparency information was supplied by the server.  
[Certificate information](#)

 Your connection to pdp7.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES\_128\_GCM and uses ECDHE\_RSA as the key exchange mechanism.

[What do these mean?](#)

gpg key: [pdp7.pub.asc](#)  
t = D869 9E3B 6AB1 63C0 AE99 FD71 84D4 4A93 17F1 1



**Join EFF!**



**ELECTRONIC FRONTIER FOUNDATION**

The **Electronic Frontier Foundation** is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, **EFF** champions user privacy, free expression, and innovation through impact litigation, policy

fingerprint =

93 17F1 138E

Certificate Viewer: pdp7.com

General Details

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

Common Name (CN)	pdp7.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	01:BE:53:8B:4F:98:12:88:04:46:47:E2:54:00:28:FB:46:B0

Issued By

Common Name (CN)	Let's Encrypt Authority X1
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Sunday, November 8, 2015 at 6:00:00 PM
Expires On	Saturday, February 6, 2016 at 6:00:00 PM

Fingerprints

SHA-256 Fingerprint	D1 98 26 91 19 35 0D 9F C1 78 D8 AF F1 32 60 B9 E7 9E A8 6F 9A E2 FE 31 27 9E DD F3 BA 66 32 F2
SHA-1 Fingerprint	19 3F 83 8C 00 B3 04 5B ED 45 3B 6A 99 00 37 AA C7 D8 CD E6



DATION

The [Electronic Frontier Foundation](#) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, [EFF](#) champions user privacy, free



## Why 90-day lifetimes for certs?

- 90 days is nothing new on the Web
- **29% of TLS transactions use 90-day certs**  
*(per Firefox Telemetry)*
- **Limit damage** of key compromise & mis-issuance
- **Encourage automation**, which is essential for ease-of-use



# Let's Encrypt

## Get Involved

- All code & protocol specifications are on GitHub
- Client software development mailing list
- CA software development mailing list
- ACME protocol dev IETF mailing list
- Community Support Forum (Discourse)