

Free SSL Certificates

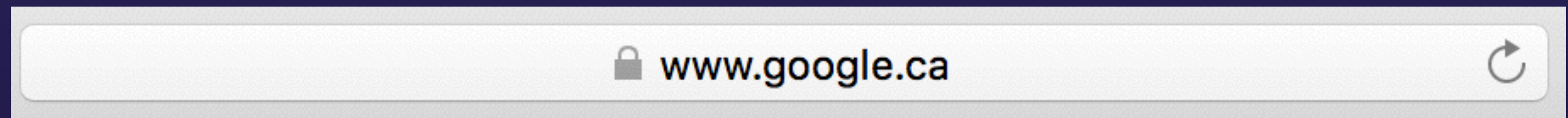


Let's Encrypt

SSL / TLS

- Trust comes from Certificate Authorities
- Certificate for each server (or wildcard for domains)

- Regular:



- EV:



SSL is expensive?

- RapidSSL: **\$49** / **\$199** wildcard
- Thawte:
 - SSL123: **\$149** / **\$745** wildcard
 - SSL Web Server: **\$199** / **\$299** EV / **\$499** wildcard
- Comodo: **\$77** / **\$99** EV / **\$405** wildcard

Want a used car with that?



EV SSL ~~\$449~~ \$99/year

Spring SALE

OFFER ENDS 01:53:27







HOURS MINUTES SECONDS

[BUY NOW](#) [Learn More](#)

It's Go Time™



WTF?

Product	Term	Unit Price	Subtotal
 Standard SSL Quantity: <input type="text" value="1"/> certificate 51% Off	2 Years 	C\$ 48.71 /yr Save C\$ 102.57	C\$ 97.41  Remove
 Standard SSL Quantity: <input type="text" value="1"/> certificate 94% Off	1 Year 	C\$ 5.99 /yr Save C\$ 94.00	C\$ 5.99  Remove

Certificate Authorities

- Supposed to check business information
- In practice, can get a certificate in minutes, no human intervention, no business documents
- What are we paying for?

What are we paying for?



LOGOS!



Let's Encrypt

- New kind of CA
- ACME protocol to check domain ownership
- Provisioning via simple software
- Standard certificates
- CRL / OCSP support

EASY!

- Two commands (FreeBSD):
 - `pkg install py27-letsencrypt`
 - `letsencrypt certonly --webroot
-w /usr/local/christodeluxe/www
-d christodeluxe.com
-d www.christodeluxe.com`

EASY!

Enter email address (used for urgent notices and lost key recovery)

|csaldanh@gmail.com

< OK >

<Cancel>

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>

EASY!

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at `/usr/local/etc/letsencrypt/live/christodeluxe.com/fullchain.pem`. Your cert will expire on 2016-07-09. To obtain a new version of the certificate in the future, simply run Let's Encrypt again.
- If you lose your account credentials, you can recover through e-mails sent to `csaldanh@gmail.com`.
- Your account credentials have been saved in your Let's Encrypt configuration directory at `/usr/local/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.
- If you like Let's Encrypt, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>
Donating to EFF: <https://eff.org/donate-le>

Apache Setup

```
<VirtualHost *:443>
```

```
    SSLEngine On
```

```
    SSLHonorCipherOrder on
```

```
    SSLCipherSuite HIGH:!aNULL:!MD5:!RC4
```

```
    SSLProxyCipherSuite HIGH:!aNULL:!MD5:!RC4
```

```
    SSLProtocol all -SSLv3
```

```
    SSLProxyProtocol all -SSLv3
```


```
    SSLCertificateFile /usr/local/etc/letsencrypt/live/christodeluxe.com/cert.pem
```

```
    SSLCertificateKeyFile /usr/local/etc/letsencrypt/live/christodeluxe.com/privkey.pem
```




```
    SSLCertificateChainFile /usr/local/etc/letsencrypt/live/christodeluxe.com/chain.pem
```


```
</VirtualHost>
```


Browsers

**Safari is using an encrypted connection to www.christodeluxe.com.**

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.christodeluxe.com.


 DST Root CA X3
↳  Let's Encrypt Authority X3
↳  www.christodeluxe.com

**www.christodeluxe.com**

Issued by: Let's Encrypt Authority X3
Expires: Saturday, July 9, 2016 at 11:18:00 AM Eastern Daylight Time
✔ This certificate is valid

► **Trust**
▼ **Details**


Subject Name	
Common Name	www.christodeluxe.com
Issuer Name	
Country	US
Organization	Let's Encrypt
Common Name	Let's Encrypt Authority X3
Serial Number	03 2C D4 20 36 3D EF 16 25 E3 2F 1E 55 8E 5E 53 D8 F0
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Sunday, April 10, 2016 at 11:18:00 AM Eastern Daylight Time
Not Valid After	Saturday, July 9, 2016 at 11:18:00 AM Eastern Daylight Time


 <https://www.christodeluxe.com>

www.christodeluxe.com

Your connection to this site is private.
[Details](#)

Permissions Connection

 Chrome verified that Let's Encrypt Authority X3 issued this website's certificate. The server did not supply any Certificate Transparency information.
[Certificate Information](#)

 Your connection to www.christodeluxe.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.

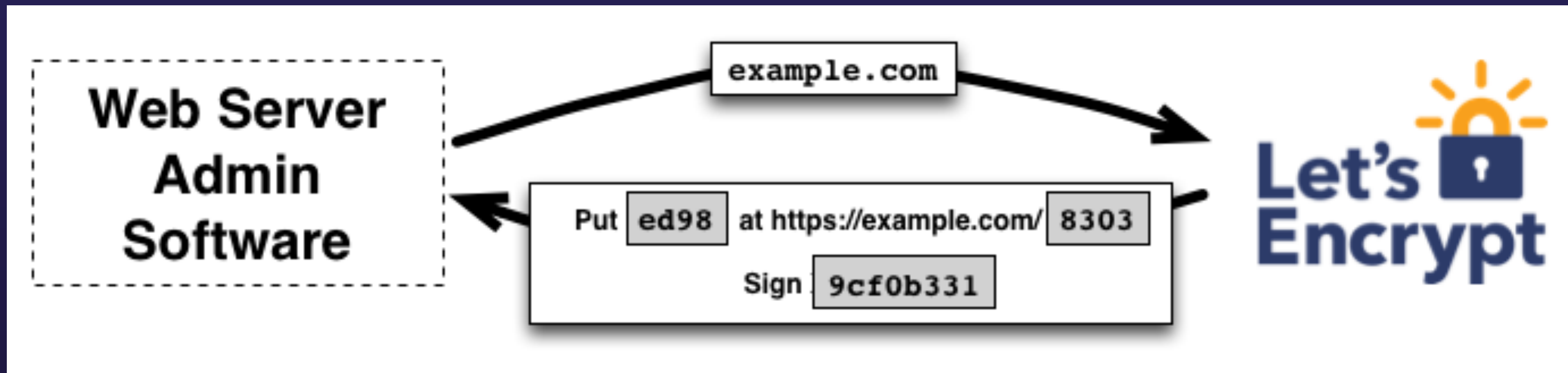
[What do these mean?](#)

Domain Validation: ACME

- Need to know you control the site
- ACME protocol to the rescue!
 - Web-based approach
 - DNS-based approach

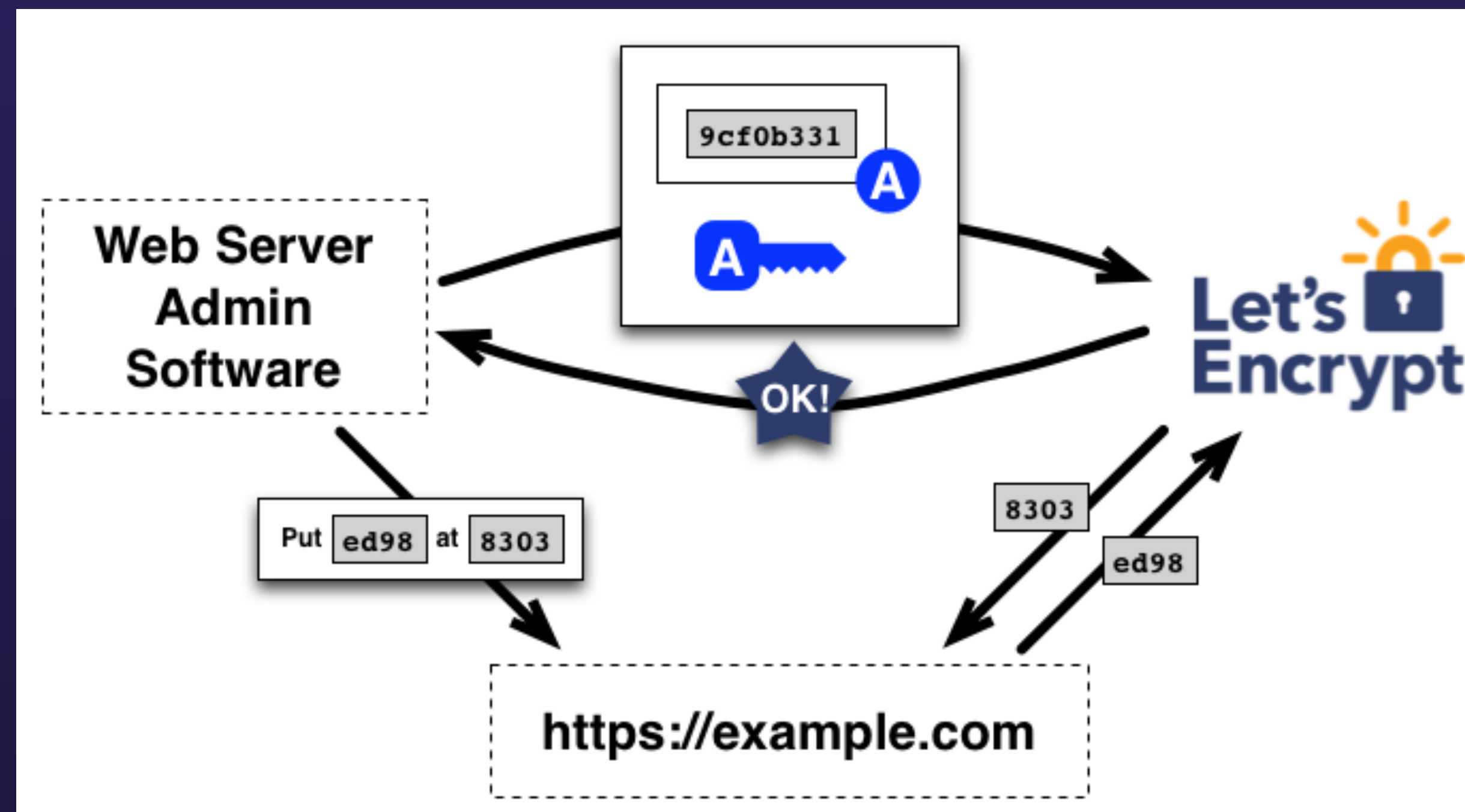
ACME - Web Validation

- CA sends a nonce (random value), client to encrypt
- CA asks for a resource to be created on the site



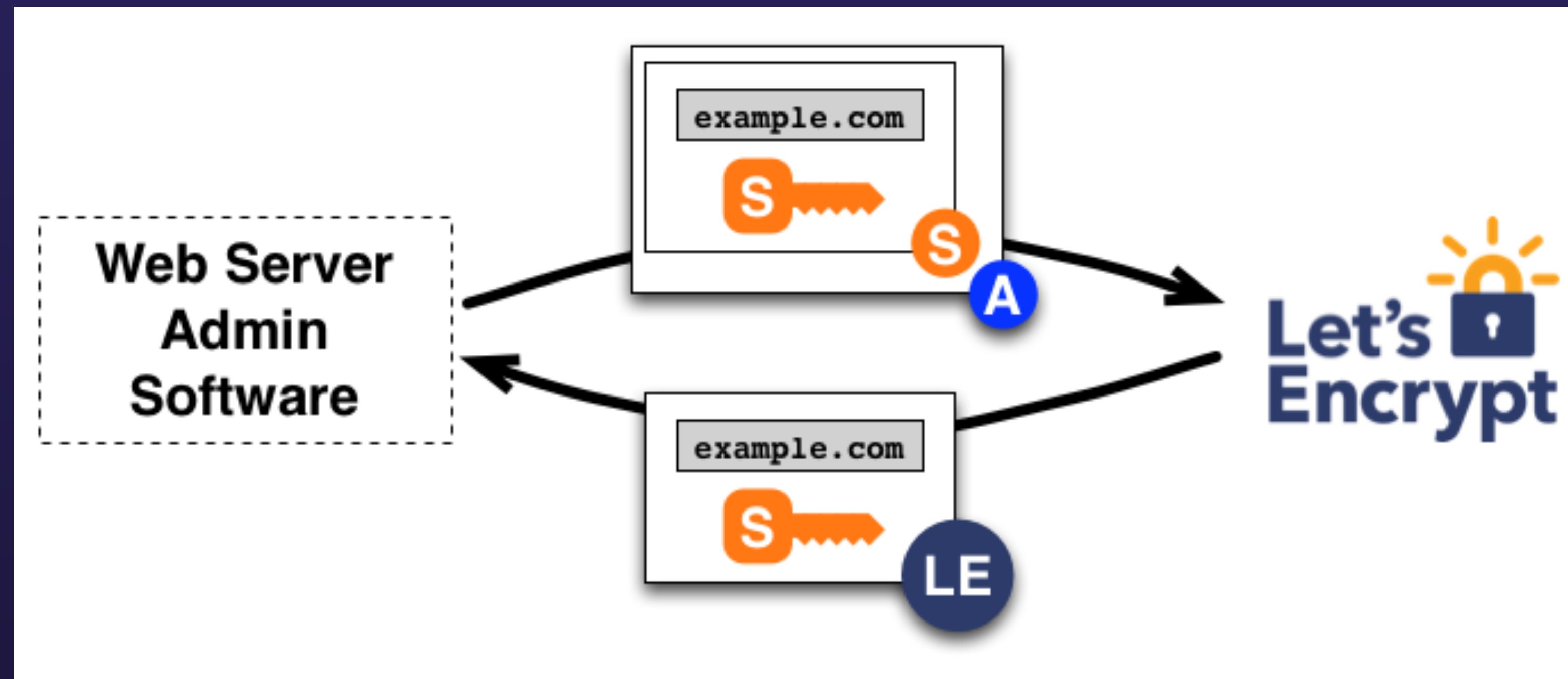
ACME - Web Validation

- client returns signed nonce, provisions resource
- CA goes to live web site, downloads resource



ACME - Web Validation

- If checks pass, client sends CSR to CA
- CA returns signed certificate



Limits

- LE issues 3-month certificates (expects regular, automated renewal)
- 100 host names per certificate
- 5 changes/week for existing host names
- 20 certs per domain per week

Browser support

✓ Firefox, Chrome

✓ IE / Windows Vista+ (XP SP3 too)

✓ Safari 4.0+, iOS 3.1+

✓ Android 2.3.6+

😱 No Blackberry, Nintendo 3DS support

SSL FTW!



Let's Encrypt