SAC057 / non-FQDN Certs

Fun with TLDs…

Warren Kumari (ICANN Beijing, 2013-04)

Background

- *https:// requires a public key, carried in a certificate.*
- *Obtain this from a Certification Authority*
- *Binds public key to identity*
- *Browser uses this to make sure it is talking to the correct server.*

Validation

- *Validation* is simply receiving a token in email at an address (webmaster@, the email address in WHOIS)*
- *Reply with the token to prove "ownership" of the domain.*

* : *Domain Validated certificates. EV / OV have more stringent validation.*

Internal Server Names

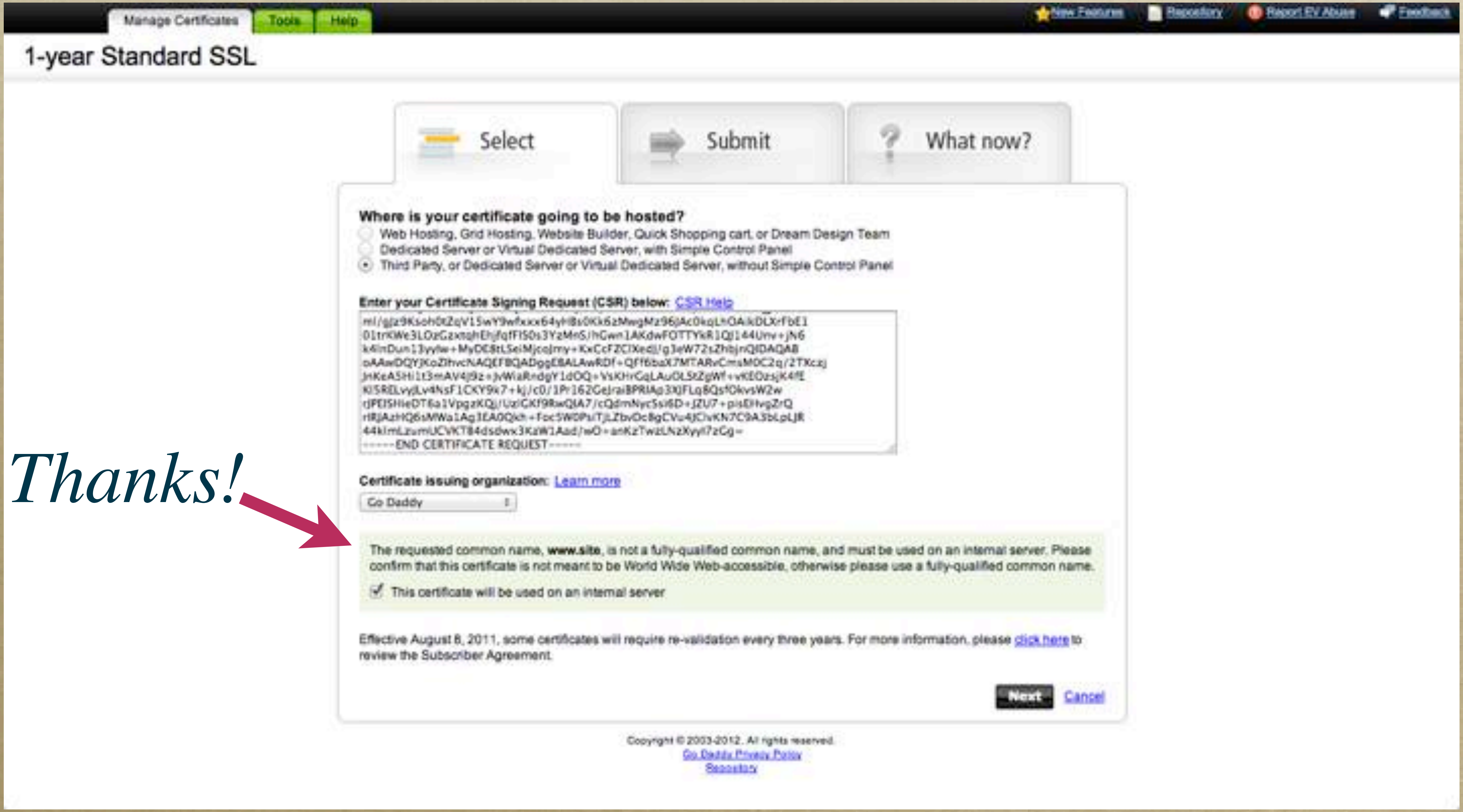
- *Designed for "internal only" type applications.*
  - *Often used by Microsoft Exchange, Active Directory.*
- *www.corp, www.accounting, mail.test*
- *Doesn't end in a TLD*
  - *can't be used on the Internet*
  - *nowhere to send the validation email*

What’s a TLD?

Certificate request

```
Certificate Request:
  Data:
   Version: 0 (0x0)
    Subject: C=US, ST=VA, L=Dulles,
O=Dulles Steel and Forge Supplies,
OU=IT - Internal WWW Site.,
CN=www.site/emailAddress=warren@kumari.net
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:da:ef:bd:d0:ee:db:...
....
```

Internal Name Certificate?



1-year Standard SSL

Where is your certificate going to be hosted?

○ Web Hosting, Grid Hosting, Website Builder, Quick Shopping cart, or Dream Design Team
○ Dedicated Server or Virtual Dedicated Server, with Simple Control Panel
● Third Party, or Dedicated Server or Virtual Dedicated Server, without Simple Control Panel

Enter your Certificate Signing Request (CSR) below: CSR Help

```
ml/gjz9Ksoh0tZqV15wY9wfxxx64yHBs0Kk6zMwgMz96jAc0kqLhOAikDLXrFbE1
01trKWe3LOzGzxtqhEhjfqfFIS0s3YzMnS/hGwn1AKdwFOTTYkR1QjI144Unv+jN6
k4InDun13yylw+MyDE8tLSeiMjcoJmy+KxCcFZClXedjI/g3eW72sZhbjnQIDAQAB
oAAwDQYJKoZIhvcNAQEFBQADggEBALAwRDf+QFf6baX7MTARvCmsM0C2q/2TXczj
JnKeASHi1t3mAV4j9z+JvWiaRndgY1dOQ+VsKHrGqLAuOL5tZgWf+vKEOzsjK4fE
KISRELvyjLv4NsF1CKY9k7+kj/c0/1Pr162GeJraiBPRIAp3XJFLq8QsfOkvsW2w
rjPEISHieDT6a1VpgzKQj/UzlGKf9RwQIA7/cQdmNyc5si6D+JZU7+pisEHvgZrQ
rIRJAzHQ6sMWa1Ag3EA0Qkh+Foc5W0Ps/TjLZbvOc8gCVu4JClvKN7C9A3bLpLJR
44kImLzumUCVKT84dsdwx3KzW1Aad/wO+anKzTwzLNzXyyI7zCg=
-----END CERTIFICATE REQUEST-----
```

Certificate issuing organization: Learn more

Go Daddy

Thanks!

The requested common name, **www.site**, is not a fully-qualified common name, and must be used on an internal server. Please confirm that this certificate is not meant to be World Wide Web-accessible, otherwise please use a fully-qualified common name.

☑ This certificate will be used on an internal server

Effective August 8, 2011, some certificates will require re-validation every three years. For more information, please click here to review the Subscriber Agreement.

Copyright © 2003-2012. All rights reserved.
Go Daddy Privacy Policy
Repository

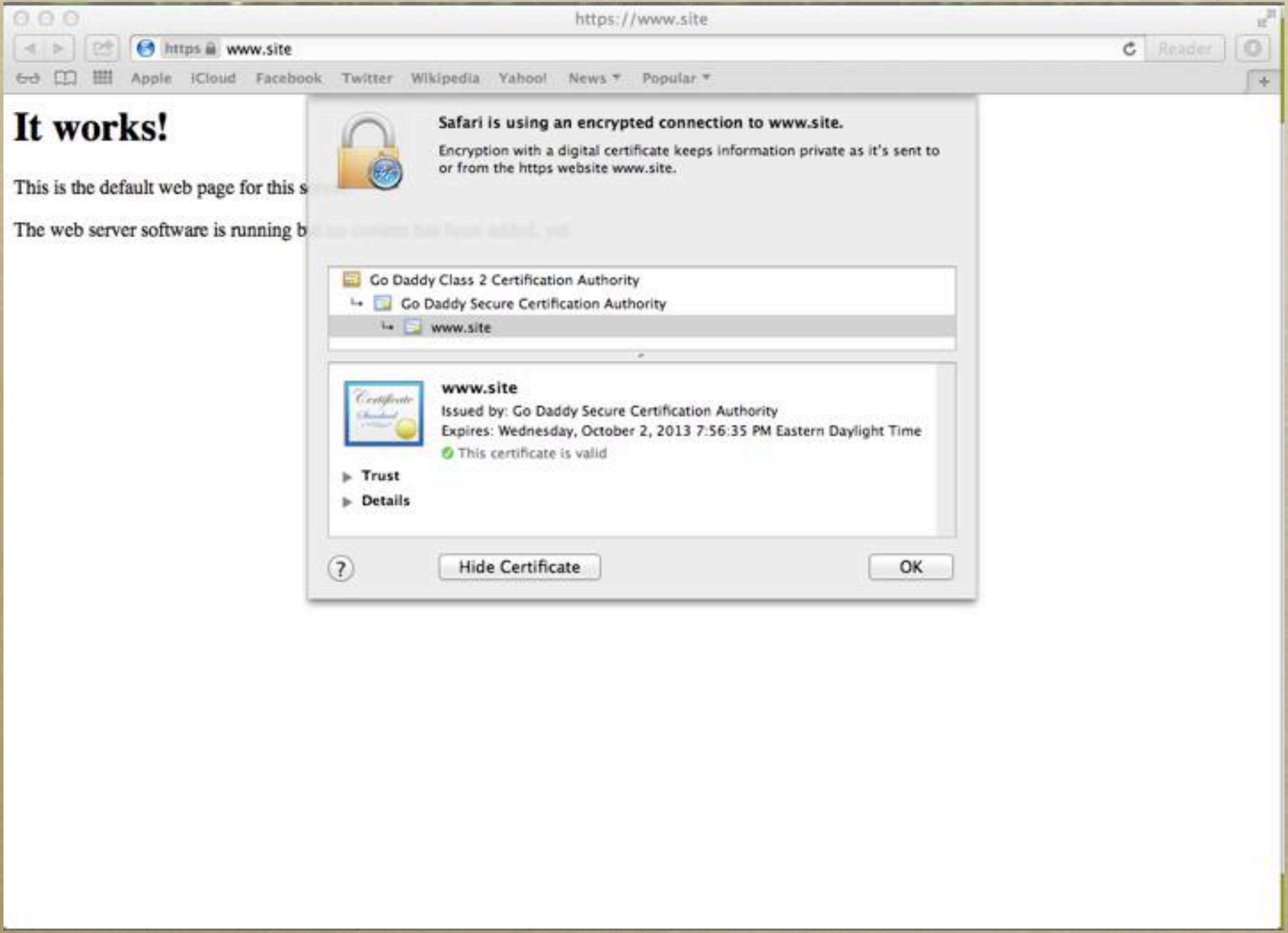
Issued Certificate

```
Data:
  Version: 3 (0x2)
  Serial Number:
    27:e7:22:63:59:11:b0
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, ST=Arizona, L=Scottsdale,
   O=GoDaddy.com, Inc., OU=http://
certificates.godaddy.com/repository, CN=Go Daddy Secure
Certification Authority/serialNumber=07969287
   Validity
     Not Before: Oct  2 23:56:35 2012 GMT
     Not After : Oct  2 23:56:35 2013 GMT
  Subject: O=www.site, OU=Domain Control Validated,
           CN=www.site
  X509v3 Subject Alternative Name:
                DNS:www.site, DNS:site
```

Testing

- *Setup a fake root*
- *Delegated .site to myself*
- *Setup a webserver, serving the cert*

Doh!



It works!

This is the default web page for this s

The web server software is running b

Safari is using an encrypted connection to www.site.

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

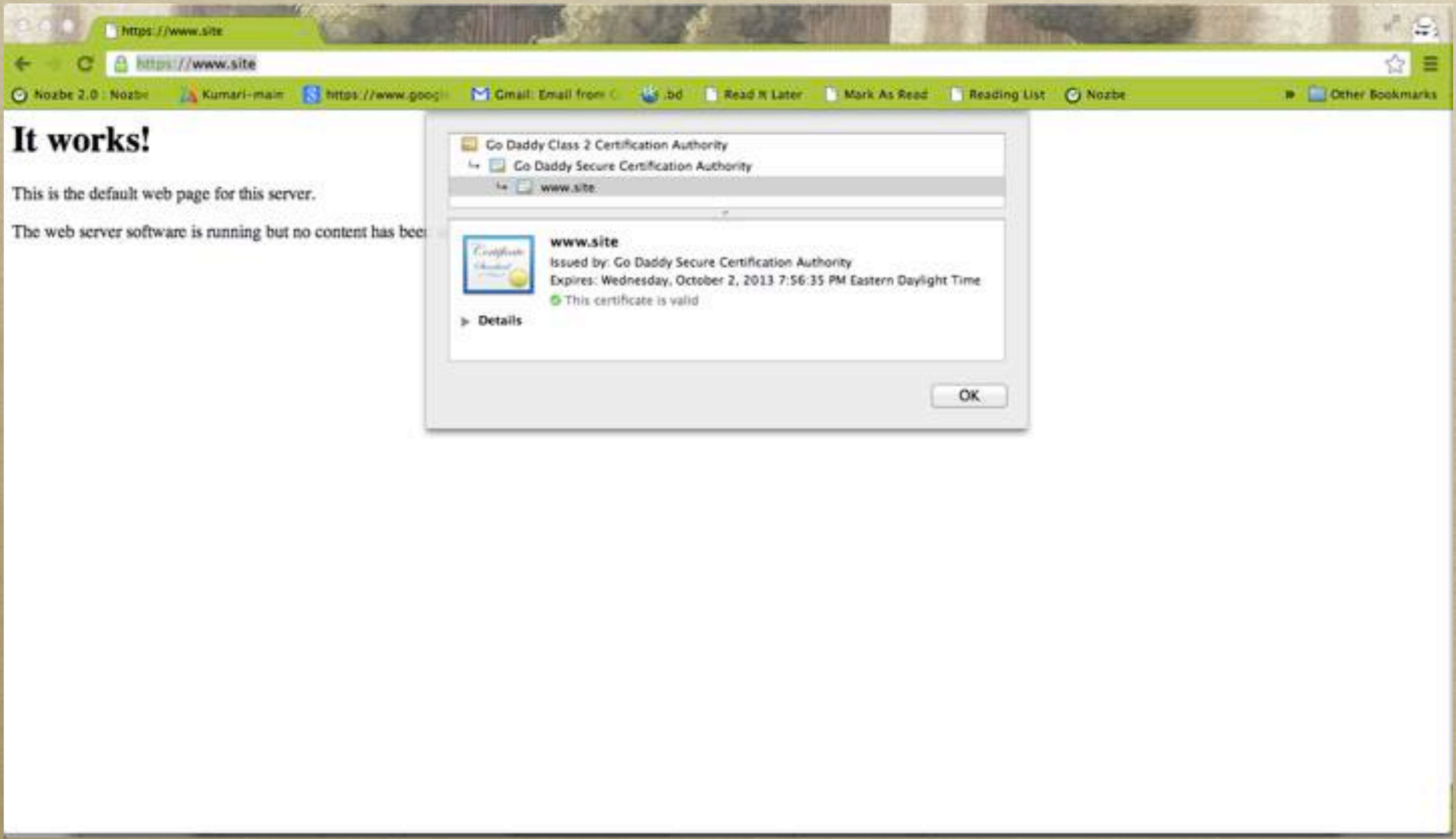
Go Daddy Class 2 Certification Authority
↳ Go Daddy Secure Certification Authority
↳ www.site

www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
✓ This certificate is valid

▶ Trust

▶ Details

Doh!



It works!

This is the default web page for this server.

The web server software is running but no content has bee

Go Daddy Class 2 Certification Authority
↳ Go Daddy Secure Certification Authority
↳ www.site

www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
This certificate is valid

▶ Details

So what?

1. *Get a certificate for something ending in an applied for TLD.*
2. *Wait for it to be delegated.*
3. *Hang out in Starbucks, or a hotel, or domain hijack, or cache-poison, or DHCP poison, or...*
4. *Present this cert, get the lock icon.*
5. *Steal banking credentials, cookies, etc*

Investigations

- *SSAC formed a work party*
- *Researched prevalence of non-FQDN certs*
    - *Using the EFF SSL Observatory data*
    - *1,053 Internal Server Name certificates ending in 63 applied-for TLD*
        - ***Lower bounds** estimate*

Investigations

- *Confidentiality issues*
- *Responsible Disclosure*
    - *Security Team*
        - *Contacted CA/B Forum*
        - *“Coordinated Vulnerability Disclosure”*

CA/B Forum

- *CA/B Forum stepped up.*
- *Already had started deprecating internal certs, but speeded things up:*
  - *Stop issuing within 30 days of each new gTLD approval*
  - *Revoke within 120 days*
    - *Unless customer proves domain ownership.*

Solved? Nope...

- *Not all CAs are members of the CA/B Forum*
  - *So not bound by these agreements*
  - *But generally trustworthy / follow guidelines*
- *Revocation ineffective**
  - *Blocking CRL / OSCP / air-gapped networks*

** : http://www.imperialviolet.org/2011/03/18/revocation.html*

Questions?