Certificate Authorities

The Shady World of Trust

Scope

- Not a talk on X.509, SSL, TLS, etc.
- More about policy on becoming CAs

What's in Scope?

- You want to want to learn more about public root CAs
- You want to become a public trusted root CA
- You want to become the next GoDaddy, Comodo, or VeriSign

Origin of Idea

- My first DEFCON, DC19
  - Shout out to Vidiot & Luna
- Moxie Marlinspike's "SSL & the future of Authenticity"

Trust Agility

"Convergence allows you to choose who you want to trust, rather than having someone else's decision forced on you. You can revise your trust decisions at any time, so that you're not locked in to trusting anyone for longer than you want."

http://convergence.io/details.html

Trust Agility

"Convergence allows you to choose who you want to trust, rather than having someone else's decision forced on you. You can revise your trust decisions at any time, so that you're not locked in to trusting anyone for longer than you want."

http://convergence.io/details.html

wait…what decision?

Origin of Idea

"Oh that whole authenticity thing...we through that in the end. It is a bit of a hand wave."

- Kipp Hickman, Netscape Engineer

Origin of Idea

"…650+ CAs trusted by Microsoft & Mozilla…"

- EFF SSL Observatory

Origin of Idea

"Certificate Authorities cannot be trusted"**

- Moxie Marlinspike

**paraphrasing...but I'm sure he said that at one point somewhere..some time...I'm sure of it.

Origin of Idea

"Certificate Authorities are such a security disaster for the entire internet. We need to build viable alternatives and quickly."

- Jacob Applebaum

https://twitter.com/ioerror/status/500663276453355552

Talk v1.0

Talk v1.0

- ???
- Usurp trust stores
- Submit a talk about becoming a CA
- Shower of applause

Let’s do it!

An Incomplete & Biased History of SSL, CAs, and more.

The ‘talk’

??? => Trust Stores => Crypto => Lolcats

The ‘talk’

??? => Trust Stores => Crypto => Lolcats

End users

The ‘talk’

??? => Trust Stores => Crypto => Lolcats

Three letter agencies

The ‘talk’

??? => Trust Stores => Crypto => Lolcats

The Moxies

The ‘talk’

??? => Trust Stores => Crypto => Lolcats

me

1994 - Netscape creates SSL 1.0
1995 - Verisign founded. Netscape publishes spec for SSL 2.0
1996 - SSL 3.0 is released.
1999 - TLS1.0 defined in RFC 2246. CRL & OCSP proposed in RFC2459
2001 - Verisign mistakenly issues a certificate for *.microsoft.com to a non-Microsoft employee
2002 - Moxie releases sslsniff
2003 - Verisign gives up .org tld
2004 - GoDaddy begins selling SSL certs
2006 - TLS 1.1 defined in RFC 4346
2008 - TLS 1.2 defined in RFC 5246
2009 - Moxie releases sslstrip
2010 - Verisign is bought by Symantec for $1.28B.
2011 - Comodo, DigiNotar, & TurkTrust issued fake certificates
2012 - Trustwave issues an intermediate CA certificate to DLP company

1994 - Netscape creates SSL 1.0
1995 - Verisign founded. Netscape publishes spec for SSL 2.0
1996 - SSL 3.0 is released.
1999 - TLS1.0 defined in RFC 2246. CRL & OCSP proposed in RFC2459
2001 - Verisign mistakenly issues a certificate for *.microsoft.com to a non-Microsoft employee
2002 - Moxie releases sslsniff
2003 - Verisign gives up .org tld
2004 - GoDaddy begins selling SSL certs
2006 - TLS 1.1 defined in RFC 4346
2008 - TLS 1.2 defined in RFC 5246
2009 - Moxie releases sslstrip
2010 - Verisign is bought by Symantec for $1.28B.
2011 - Comodo, DigiNotar, & TurkTrust issued fake certificates
2012 - Trustwave issues an intermediate CA certificate to DLP company

How to become a CA

- Generate paperwork
- Generate certificates
- Get audited
- Apply to major trust stores
- Done!

Docs

- Public documentation on policies:
  - Certificate Policy (CP)
  - Certification Practice Statement (CPS)

CP/CPS

- Defines how the CA is setup physically, hierarchy, technical & physical controls
- Defines how certificates are generated, revoked, etc.
- Defines how identities are authenticated
- Defined in RFC 3647

“Good artists copy, great artists steal”

“Good artists copy, great artists steal”

- Steve Jobs

“Good artists copy, great artists steal”

- Steve Jobs
- Pablo Picasso

CP/CPS

- Verisign (aka Symantec): 87 pages
- Starfield (aka GoDaddy): 90 pages
- Trustis: 42 pages

Generate Certificates

Generate Certificates

Quick & dirty demo...

Generate Certificates

- Need to manage certificates
  - Certificate management
  - Accepting requests
  - Revocation (OCSP & CRL)*

Revocations*

- OCSP vs CRL
- Key Pinning

Get Audited!

Audits

- Third party verification of controls
- Requirement for Trust Stores
- Only a handful of audits are recognized

Audits

- WebTrust's "Principles and Criteria for Certification Authorities"
- Done by: KPMG, Ernst & Young, Deloitte, and more

Audits

- WebTrust is a Canadian Accounting company
- Requires auditors to be a part of their “Trust Services Program”

Audits

Signing Up for the Trust Services Program

Common Qualifications Required For Seal Usage

Before a practitioner may issue any of the Trust Services Program seals to its clients, the practitioner must:

1. Be or become licensed (for more information on how to obtain a license, see the Understanding and Implementing Trust Services guide or email webmaster@webtrust.org in the U.S. or webtrust@cica.ca in Canada).
2. Self-assess competence in the subject area and determine what, if any, additional training and/or assistance is required to perform the engagement.

For each client, the practitioner will need to:

1. Complete an examination/audit level Trust Services engagement using the appropriate Trust Services Principles and Criteria as suitable criteria.
2. Sign an unqualified opinion for the engagement.
3. Enroll the client and issue a seal using the Seal Management System.
4. Have the client's organization post the seal to its web site.
5. Pay an administrative fee for the seal that has been issued.

http://www.webtrust.org/signing-up-for-the-trust-services-program/item64422.aspx

Audits

Signing Up for the Trust Services Program

Common Qualifications Required For Seal Usage

Before a practitioner may issue any of the Trust Services Program seals to its clients, the practitioner must:

1. Be or become licensed (for more information on how to obtain a license, see the Understanding and Implementing Trust Services guide or email webmaster@webtrust.org in the U.S. or webtrust@cica.ca in Canada).
2. Self-assess competence in the subject area and determine what, if any, additional training and/or assistance is required to perform the engagement.

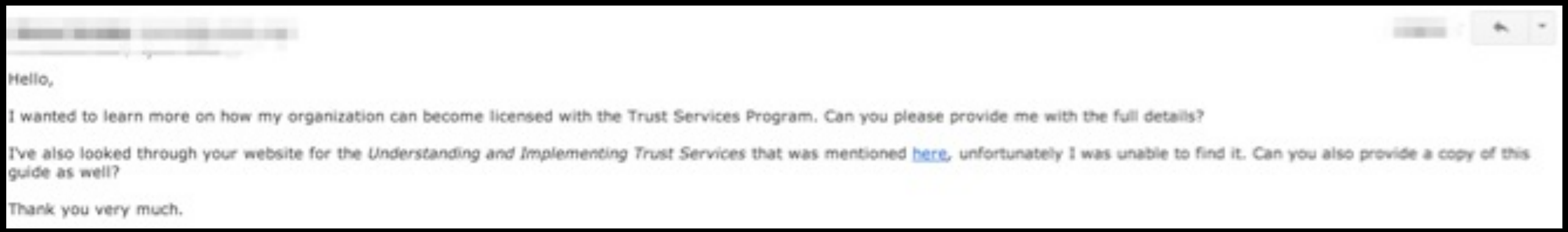
For each client, the practitioner will need to:

1. Complete an examination/audit level Trust Services engagement using the appropriate Trust Services Principles and Criteria as suitable criteria.
2. Sign an unqualified opinion for the engagement.
3. Enroll the client and issue a seal using the Seal Management System.
4. Have the client's organization post the seal to its web site.
5. Pay an administrative fee for the seal that has been issued.

http://www.webtrust.org/signing-up-for-the-trust-services-program/item64422.aspx

Audits

Audits



Hello,

I wanted to learn more on how my organization can become licensed with the Trust Services Program. Can you please provide me with the full details?

I've also looked through your website for the *Understanding and Implementing Trust Services* that was mentioned here, unfortunately I was unable to find it. Can you also provide a copy of this guide as well?

Thank you very much.

Audits

Hello,

I wanted to

I've also loo

guide as wel

Thank you v

wide a copy of this

Good morning Osman

After reviewing your email below to can you please confirm the following :

- Do you wish to engage an Accounting firm for your company to become certified, or do you wish to become a Practitioner of Trust Services.
- From your website I gathered that you are not an Accounting firm, can you please confirm ?

Once I have more information I can better help to provide any required information you may need.

Audits

Hello,

I wanted to

I've also loo

guide as wel

Thank you v

wide a copy of this

Good morning Osman

After reviewing your email below to can you please confirm the following :

-

-

ust Services.

O Hi Osman

My apologies for the delay, Can you please confirm if your firm is a member of the AICPA or a state society of accountants?

Many Thanks

Audits

Hello,

I wanted to

I've also loo

guide as wel

Thank you v

wide a copy of this

Good morning Osman

After reviewing your email below to can you please confirm the following :

-

-

ust Services.

Hi Osman

My apologies for the delay, Can you please confirm if your firm is a member of the AICPA or a state society of accountants?

Good morning Osman

Unfortunately it is a requirement that you are a member of the Institute in your jurisdiction in order to become a Practitioner of Trust Services.

Talk v2.0

Talk v2.0

- ???
- Usurp trust stores
- Submit a talk about becoming a CA
- Shower of applause

Talk v2.0

- ???
- ~~Usurp trust stores~~
- Submit a talk about becoming a CA
- ~~Shower of applause~~

Trust Stores?

- Major trust stores:
  - Apple
  - Microsoft
  - Mozilla
- Covers ~90.3% browsers, but probably closer to 99%

Apple Trust Store

- Scope: All Apple products*
  - * iOS: ?!?
- Audit: WebTrust Audit or equivalent
- Updates: Through Apple's software update mechanisms
- Members: 181 CAs

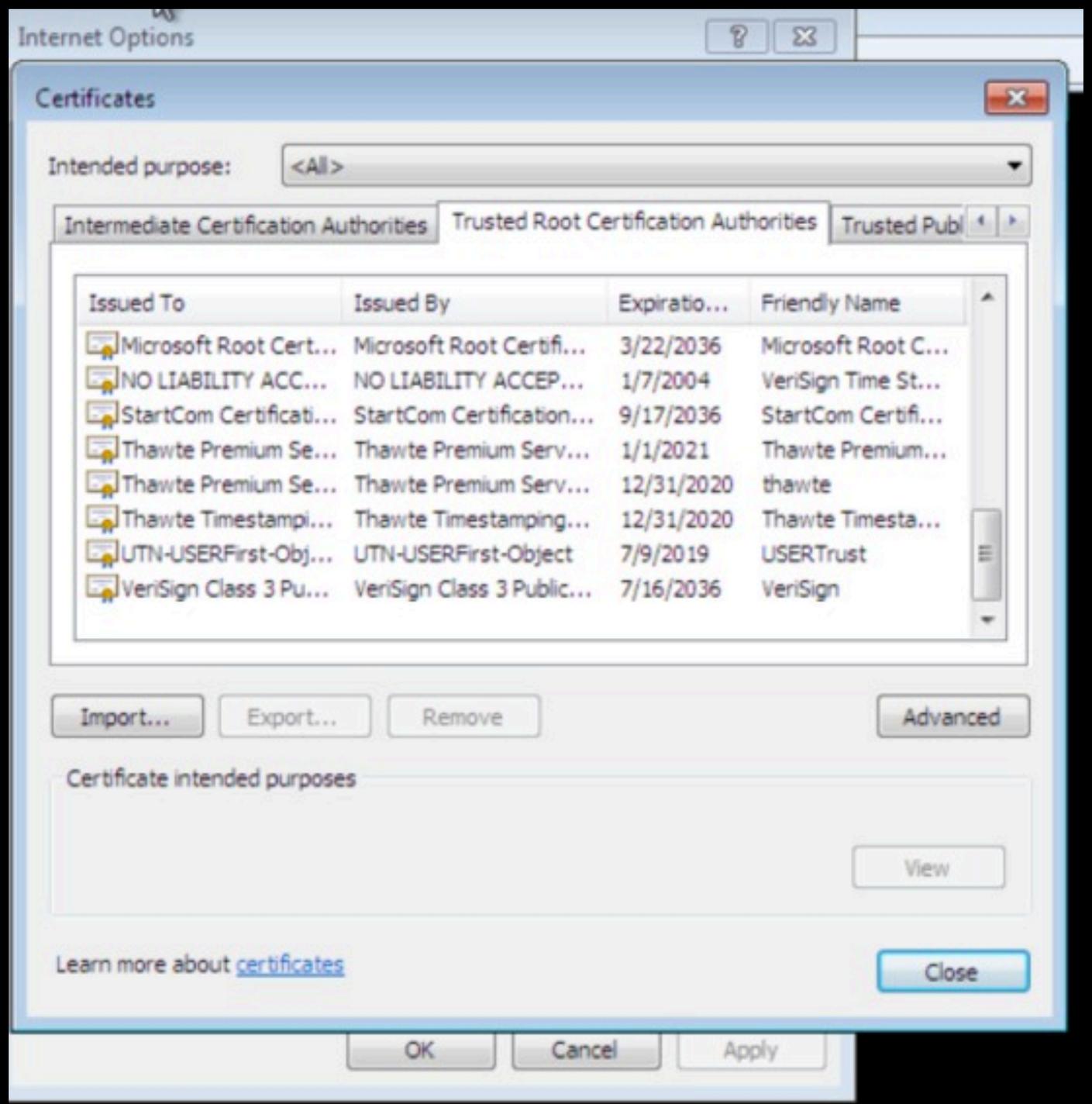
Microsoft Trust Store

- Scope: All MS products
- Audit: WebTrust, ETSI, or equivalent
- Updates: It depends
- Members: 353 CAs

Microsoft Trust Store

- Defined in KB931125
- Updates:
  - XP: Windows Update
  - Windows Vista+: *Demo!*

Demo God Backup



Demo God Backup

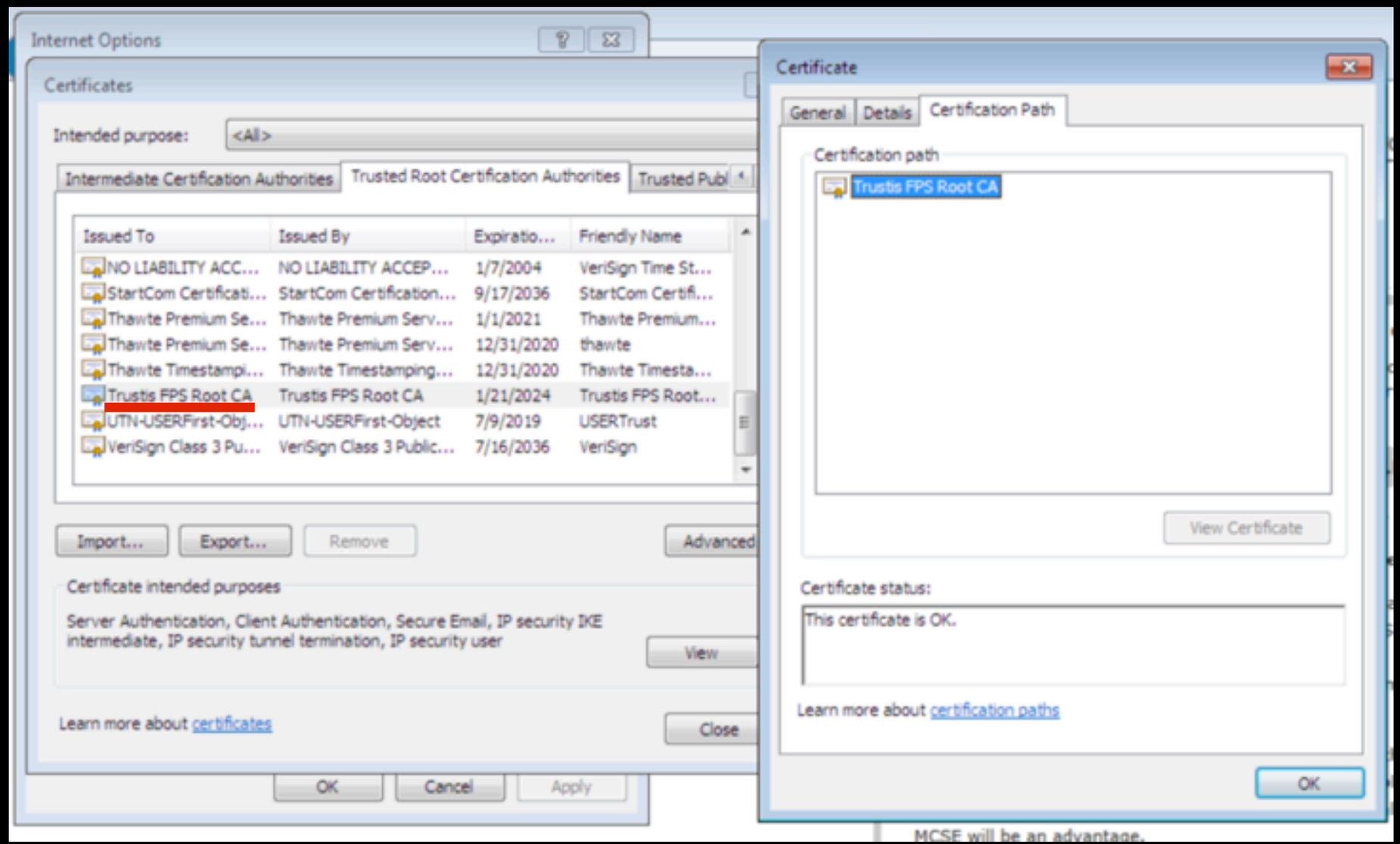
Demo God Backup

```
⊞ Frame 726: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
⊞ Ethernet II, Src: Vmware_e3:e4:0f (00:0c:29:e3:e4:0f), Dst: Vmware_f9:a8:b0 (00:50:56:f9:a8:b0)
⊞ Internet Protocol Version 4, Src: 172.16.70.153 (172.16.70.153), Dst: 172.16.70.2 (172.16.70.2)
⊞ User Datagram Protocol, Src Port: 51440 (51440), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 727]
    Transaction ID: 0xca0a
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ update.microsoft.com: type A, class IN
        Name: update.microsoft.com
        Type: A (Host address)
        Class: IN (0x0001)
```

Demo God Backup

```
⊞ Frame 726: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
⊞ Ethernet II, Src: Vmware_e3:e4:0f (00:0c:29:e3:e4:0f), Dst: Vmware_f9:a8:b0 (00:50:56:f9:a8:b0)
⊞ Internet Protocol Version 4, Src: 172.16.70.153 (172.16.70.153), Dst: 172.16.70.2 (172.16.70.2)
⊞ User Datagram Protocol, Src Port: 51440 (51440), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 727]
    Transaction ID: 0xca0a
.......
.2.8.......2.............update.microsoft.com.
.................
....M..Q..W
.X....R-...4.....tj..D.t0.. ......(e.v)x./x..qp.././f...Pk:w.....................0...0..........3.................0
..*.H..
.....0..1.0...U....US1.0...U...
washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1,0*..U...#Microsoft Update Secure Server CA 10..
120706235350Z.
131006235350Z0w1.0...U....US1.0...U...
washington1.0...U....Redmond1.0...U.
..Microsoft1.0...U....WUPDS1.0...U....update.microsoft.com0.."0
..*.H..
..........0..
.......y....|.....H.T.9.!w?..).C.....w....._.8.HX........j.s....6.../h..qY.X@..."Iqf..?t...K.DnGNu..6
k...P....H.....b.V......]....|._Ek:...{v.....yul..d..(.............;.....Q...T...KgJ$:?<E}i.a.. ..N.A.G....7.7..q.......V..N(..9....+.....
(.g........T0..P0...U..........0...U.%..0
..+.......0...U........)N
d:.iPQgQ..JP;.C0...U.#..0........o..0.n*]l#e.t~.0f..U..._0]0[.Y.W.Uhttp://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Secure%20Serve
+........g0e0c..+.....0..Whttp://www.microsoft.com/pkiops/certs/Microsoft%20Update%20Secure%20Server%20CA%201.crt0...U.......0.0
..*.H..
............
..L..i..79.....`..{N2.^.._.#...{....e....V..a....*....s{F'..R..v.
..WZO.B......NP..
;.9.......@.<.+.w.!w....P..........8....!.(9S..4..Q:...][a.;..I....a..;i..g.m.
....q!.....b...T.q.8."6...x..fC...].&.9..i..GAo.:..%(g.L_6.b. _..![...y...i..uh...L+.^S|.P|x.....#Zk.r.H..e...BC'._.P/
p..u.i..M.6Sn...|.....m.......R.Yy.._8.j.".*q....B....}.i.b.....Q....7....d.O...o..e.\.Op.6... BZH........X)k8H0.E..V..:{....2p3.
[.../......Q..h.O....9.....xur...I.^p..K.t..P!$.3]!..w!..)V....(.=.73.%..6.u.....>.&...S9..m5........0...0..........3...4..v.G.uC.....40
..*.H..
.....0_1.0..
..&...,d....com1.0..
..&...,d....microsoft1-0+..U...$Microsoft Root Certificate Authority0..
120531034900Z.
210509232813Z0..1.0...U....US1.0...U...
washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1,0*..U...#Microsoft Update Secure Server CA 10.."0
..*.H..
```

Demo God Backup



Microsoft Trust Store

Specific information sent or received: The Update Root Certificates feature sends a request to http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en, asking for the current list of root certification authorities in the Microsoft Root Certificate Program. If the root CA that is not directly trusted is named in the list, Update Root Certificates obtains the certificate for that root CA and places it in the trusted certificate store on the user's computer. No user authentication or unique user identification is used in this exchange.

Encryption, privacy, and storage: When requests or certificates are sent to or from Update Root Certificates, no encryption is used. Microsoft does not track access to the list of trusted authorities that it maintains on the Windows Update Web site.

Mozilla Trust Store

- Scope: Mozilla, OSS and more
- Audit: WebTrust, ETSI, or equivalent
- Updates: Package updates
- Members: 57 CAs

Application to Mozilla CA program

Example #1

- Trustis Root CA Certificate
- http://www.trustis.com/trustis-digital-certification.htm

2006-01-20 Bug #324126 is filed

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items
2010-11-15 The inclusion of the CA is added to the "Pending" queue.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items
2010-11-15 The inclusion of the CA is added to the "Pending" queue.
2012-01-10 The CA now open for discussion.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items
2010-11-15 The inclusion of the CA is added to the "Pending" queue.
2012-01-10 The CA now open for discussion.
2012-03-27 Comment period is over. Three people commented and caught crucial issues (ambiguous statements in policies, CP/CPS docs were not public, etc.)

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items
2010-11-15 The inclusion of the CA is added to the "Pending" queue.
2012-01-10 The CA now open for discussion.
2012-03-27 Comment period is over. Three people commented and caught crucial issues (ambiguous statements in policies, CP/CPS docs were not public, etc.)
2012-03-27 A preliminary approval is given.

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items
2010-11-15 The inclusion of the CA is added to the "Pending" queue.
2012-01-10 The CA now open for discussion.
2012-03-27 Comment period is over. Three people commented and caught crucial issues (ambiguous statements in policies, CP/CPS docs were not public, etc.)
2012-03-27 A preliminary approval is given.
2012-04-04 Final approval is given

2006-01-20 Bug #324126 is filed
2006-07-05 Mozilla acknowledges request and begins process of identifying missing pieces of information
2007-03-02 Mozilla notes that correspondences should be in plaintext in the bug for the public record
2007-04-18 Application is put on hold due to lack of Audit data on the organization
2007-05-23 The "Pending CA" process begins as all of the requested information is collected. Though it was noted the audit done was three years old.
2007-05-24 The company responds saying that "As there has been no change to the assertions nor changes to the operational policies/procedures supporting them there is no requirement to undergo another audit."
2007-06-01 Mozilla identifies that the CA audit was only intended for internal reference by Trustis and not for distribution to outside entities..whoops.
2008-07-21 The company identifies ambiguous wording in Mozilla's CA policy and decides to abandon WebTrust audit and goes for ETSI standards instead.
2008-08-01 The company says they've completed the audit.
2008-08-07 Mozilla identifies that the audit was in fact from 2004.
2010-03-03 Mozilla notes there hasn't been any updates on the audit for over a year.
2010-03-04 Company notes they will be going for WebTrust again.
2010-07-09 A new bug is filed, #577665
2010-07-16 "Bug" is accepted by Mozilla and additional questions are asked.
[back and forth about additional missing items
2010-11-15 The inclusion of the CA is added to the "Pending" queue.
2012-01-10 The CA now open for discussion.
2012-03-27 Comment period is over. Three people commented and caught crucial issues (ambiguous statements in policies, CP/CPS docs were not public, etc.)
2012-03-27 A preliminary approval is given.
2012-04-04 Final approval is given
2012-09-14 Code changes made and submitted in NSS. Trustis is now an approved root certificate authority

Example #1

- Highlights
  - Total time: 6 years, 7 months, 25 days
  - Independent verification: five people
  - Trust stores? Mozilla, Microsoft, Apple, & iOS

Example #2

- Honest Achmed's Used Cars and Certificates
- https://bugzilla.mozilla.org/show_bug.cgi?id=647959

Misc. Trust Stores

- Linux:
  - Debian/Ubuntu: ca-certificates package
  - Redhat: ???, but maybe NSS*
  - Fedora: NSS
- iOS: Unknown**

* *https://bugzilla.redhat.com/show_bug.cgi?id=146818*
** *https://support.apple.com/kb/HT5012*
*** *https://code.google.com/p/android/issues/detail?id=57624*

tl;dr

- Write up paperwork...
- Become an auditor or get audited...
- Apply to a program
- Wait ~1-2 years for updates to propagate
- $$$

Next Steps

- Dive deeper into MS's root update
- Get involved
  - https://wiki.mozilla.org/CA:Schedule
  - https://wiki.mozilla.org/CA:CertificatePolicyV2.2

Next Steps

- Buy certificates from vendors and then..
- Test:
  - Identity requirements
  - Revocation speed
  - ....?

Next Steps

- Symantec: $399 + $995 (EV)
- Comodo: $64.95 + $359 (EV)
- GoDaddy: $59.99 + $99.99 (EV)
- GlobalSign: $249 + $899 (EV)
- **Total: $3,125.93 + tax**

Thanks to...

- Moxie for his talk that sparked the idea
- Black Lodge Research
- Folks that convinced me this was a decent talk

Q&A

Random Find...

- “Remove inactive RSA security 1024 v3 root”
- https://bugzilla.mozilla.org/show_bug.cgi?id=549701

Random Facts!

- Top CA vendors:
  - Symantec Group (GeoTrust, Thawte, Verisign, TrustCenter) 40.6%
  - Comodo 27.4%
  - Go Daddy Group (GoDaddy, Starfield) 13.5%
  - GlobalSign 9.3%
  - **Total: 90.8%**

source: http://w3techs.com/technologies/overview/ssl_certificate/all

Random Facts!

- VeriSign classes:
  - Class 1: Low assurance, Individuals
  - Class 2: Medium, Individuals & Organizations
  - Class 3: High, Companies
  - Class 4: Not used

References

Mozilla's Included Certificate List: https://www.mozilla.org/projects/security/certs/included/
Included CA certs in Mozilla: https://docs.google.com/spreadsheet/pub?key=0Ah-tHXMAwqU3dGx0cGFObG9QM192NFM4UWNBMlBaekE&single=true&gid=1&output=html
Trustis CA in Mozilla: https://www.mozilla.org/projects/security/certs/included/#Trustis
The EFF SSL Observatory https://www.eff.org/observatory
SSL & The Future of Authenticity http://www.thoughtcrime.org/blog/ssl-and-the-future-of-authenticity/
Netcraft's SSL Server Survey: https://ssl.netcraft.com/ssl-sample-report/
Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL http://files.cloudprivacy.net/ssl-mitm.pdf