Innovative uses as result of DNSSEC

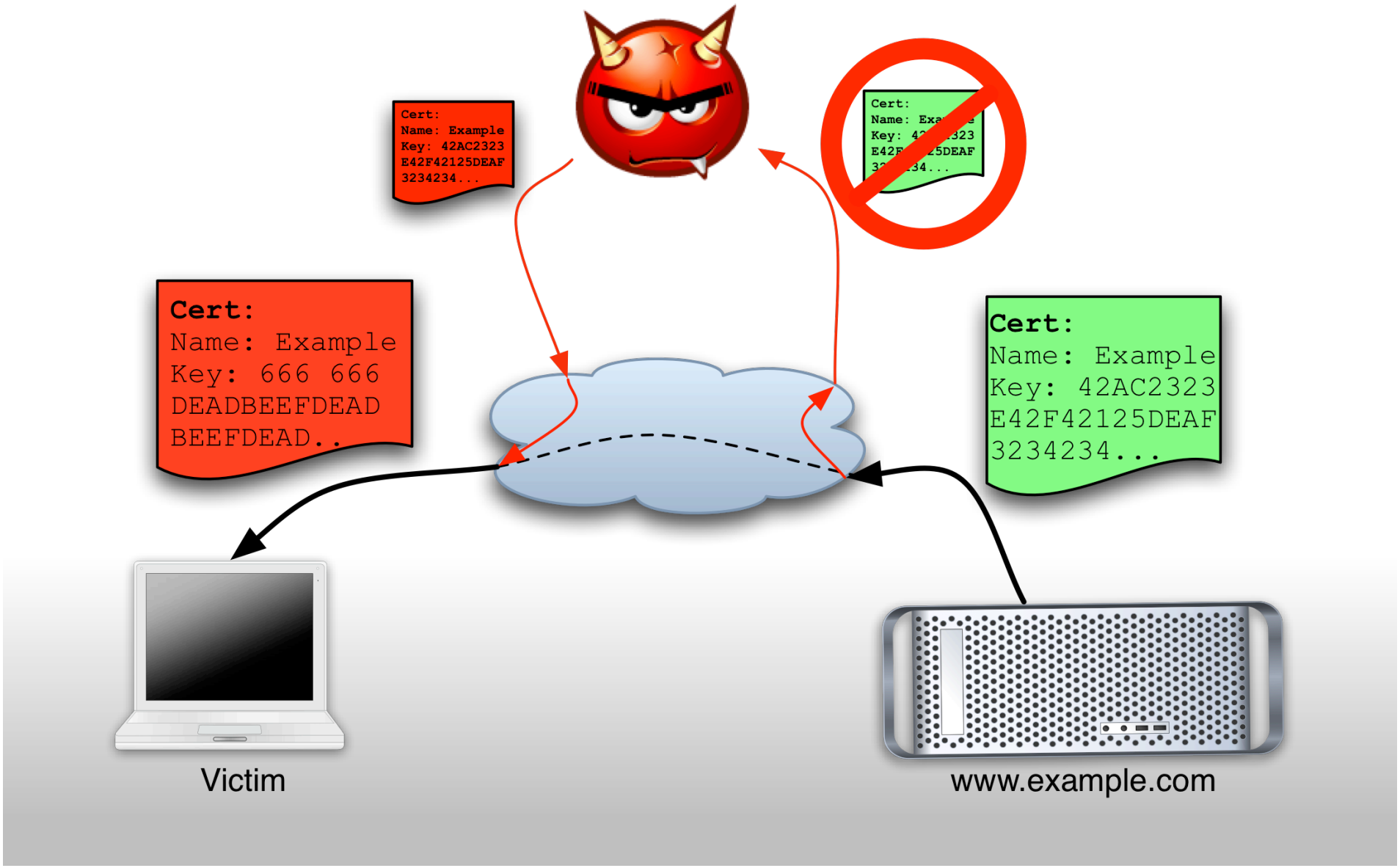
AKA: Some happenings in the DANE* WG in the IETF.

* DNS-based Authentication of Named Entities

Some background...

- When you connect to https://www.example.com you use SSL (actually TLS) to secure your connection.
- Need a public key.
- Carried in a PKIX cert.
- Need to make sure it's the **right** cert.

MITM - Man In The Middle



Public Key Infrastructure

- example.com generates public / private keypair.
- Certificate Signing Request (CSR):
  - Public part of the key
- Ships the CSR off to a Certificate Authority (CA)
- CA (usually) contacts example.com and verifies the info.
- CA issues a certificate:
  - Public part of the key
  - Hostname
  - CA's Signature.

CA's signature binds the key and hostname together and prevents tampering.

Relying Party (this is you!)

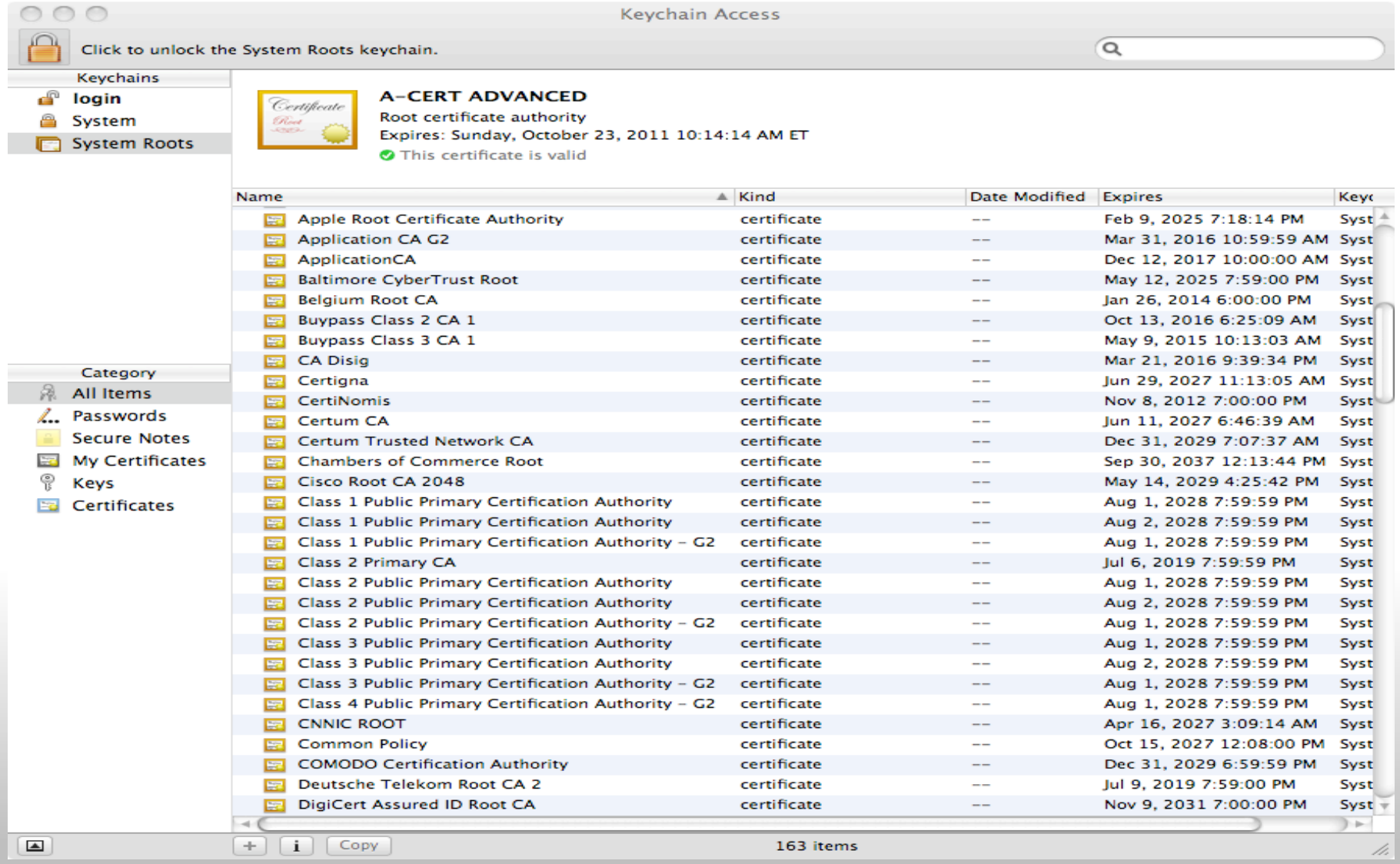
- Download the cert.
- Check that the hostname matches.
- Check a bunch of other bits in the cert that are important, just not important for this discussion :-).
- Check that the signature is valid.
- **Connect!**

Have we actually **solved** anything yet?

- Initial problem was that we didn't have a way to validate the key provided really is for example.com
- CA has signed a certificate binding the key and name together -- but, to verify the signature we need to know the CA's key....
- Well, the CA (root certificates) are basically trust anchors, just like the DNSSEC IANA trust anchor.
- Come preconfigured in your browser and your operating system.
- You inherently trust the preconfigured CAs.

Apple OSX TA Store

163 items....



Mozilla (Firefox)

155 items....

BuiltInCAs-January-2011 : Sheet1

Organization	Organizational Unit	Common Name or Certificate Name	From	To	Modulus	Signature Algorithm
(c) 2005 TÜRKTRUST Bilgi İletişim ve Biliş		TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcıs	2005 May 13	2015 Mar 22	2048	SHA-1
AC Camerfirma SA CIF A82743287	http://www.chambersign.org	Global Chambersign Root	2003 Sep 30	2037 Sep 30	2048	SHA-1
AC Camerfirma SA CIF A82743287	http://www.chambersign.org	Chambers of Commerce Root	2003 Sep 30	2037 Sep 30	2048	SHA-1
AC Camerfirma S.A.		Chambers of Commerce Root - 2008	2008 Aug 1	2038 Jul 31	4096	SHA-1
AC Camerfirma S.A.		Global Chambersign Root - 2008	2008 Aug 1	2038 Jul 31	4096	SHA-1
AddTrust AB	AddTrust TTP Network	AddTrust Class 1 CA Root	2000 May 30	2020 May 30	2048	SHA-1
AddTrust AB	AddTrust External TTP Network	AddTrust External CA Root	2000 May 30	2020 May 30	2048	SHA-1
AddTrust AB	AddTrust TTP Network	AddTrust Public CA Root	2000 May 30	2020 May 30	2048	SHA-1
AddTrust AB	AddTrust TTP Network	AddTrust Qualified CA Root	2000 May 30	2020 May 30	2048	SHA-1
America Online Inc.		America Online Root Certification Authority 1	2002 May 27	2037 Nov 19	2048	SHA-1
America Online Inc.		America Online Root Certification Authority 2	2002 May 27	2037 Sep 29	4096	SHA-1
AOL Time Warner Inc.	America Online Inc.	AOL Time Warner Root Certification Authority 1	2002 May 28	2037 Nov 20	2048	SHA-1
AOL Time Warner Inc.	America Online Inc.	AOL Time Warner Root Certification Authority 2	2002 May 28	2037 Sep 28	4096	SHA-1
AS Sertifitseerimiskeskus		Juur-SK	2001 Aug 30	2016 Aug 26	2048	SHA-1
		Autoridad de Certificacion Firmaprofesional CIF A62	2001 Oct 24	2013 Oct 24	2048	SHA-1
		Autoridad de Certificacion Firmaprofesional CIF A62	2009 May 20	2030 Dec 31	4096	SHA-1
Baltimore	CyberTrust	Baltimore CyberTrust Root	2000 May 12	2025 May 12	2048	SHA-1
Buypass AS-983163327		Buypass Class 2 CA 1	2006 Oct 13	2016 Oct 13	2048	SHA-1
Buypass AS-983163327		Buypass Class 3 CA 1	2005 May 09	2015 May 09	2048	SHA-1
Certplus		Class 2 Primary CA	1999 Jul 07	2019 Jul 06	2048	SHA-1
certSIGN	certSIGN ROOT CA	certSIGN ROOT CA	2006 Jul 04	2031 Jul 04	2048	SHA-1
Chunghwa Telecom Co., Ltd.	ePKI Root Certification Authority	ePKI Root Certification Authority	2004 Dec 19	2034 Dec 19	4096	SHA-1
CNNIC		CNNIC ROOT	2007 Apr 16	2027 Apr 16	2048	SHA-1
COMODO CA Limited		COMODO ECC Certification Authority	2008 Mar 05	2038 Jan 18	ECC	ECC
Comodo CA Limited		AAA Certificate Services	2003 Dec 31	2028 Dec 31	2048	SHA-1
Comodo CA Limited		Secure Certificate Services	2003 Dec 31	2028 Dec 31	2048	SHA-1
Comodo CA Limited		Trusted Certificate Services	2003 Dec 31	2028 Dec 31	2048	SHA-1
COMODO CA Limited		COMODO Certification Authority	2006 Nov 30	2029 Dec 31	2048	SHA-1
ComSign		ComSign Secured CA	2004 Mar 24	2029 Mar 16	2048	SHA-1
ComSign		ComSign CA	2004 Mar 24	2029 Mar 19	2048	SHA-1
Cybertrust, Inc		Cybertrust Global Root	2006 Dec 15	2021 Dec 15	2048	SHA-1

Windows / Internet Explorer

Total....

Including all of the root certificates and the certificates that they have signed that allow others to sign, and certificates that **they** have signed that allow others to sign and....

~ 1,400.

Yay! More choice is good!

No.

- When a user validates a cert, they have no way of knowing which CA should have signed it.
- Issues:
  - Malicious CA
  - Incompetent CA
  - Compelled CA.

Small chance, big risk.

DANE WG

- The big issues are way too many trust anchors...

- DNSSEC has one trust anchor and:
  - It's free.
  - It provides the ability to securely publish information.
  - Only the "domain owner" can publish at a node.
  - There is an easy discovery mechanism: the DNS itself!
  - Supports Authenticated Denial of Existence.

DANE - Leveraging DNSSEC

- Take your existing cert.
- Calculate the hash ("fingerprint").
- Publish this in the DNS (in a TLSA RR), protected with DNSSEC.
- Relying parties grab the cert, compute the hash and compare it to a TLSA record.

If they match, all is good...

If not, something evil is afoot...

* Image by Martin Cathrae, http://www.flickr.com/photos/suckamc/ (CC BY-SA 2.0)

But wait... there's more...

- In order to get a (DV) cert for a domain, all you need to do is prove you control the domain.
- Usually this is verified by proving you can receive email at (a specific address) at the domain.
- Anyone who controls the DNS for a domain can control where the mail for the domain goes.
- (Ability to control DNS for a domain) == (Ability to get cert for that domain).
- A rogue DNS admin can get a certificate for domains he administers.

What exactly does the CA do again?

- CA's signature binds the key to the hostname.
- The work in DANE will allow a site to generate and (self-sign) a certificate and publish the cert information in the DNS.
- As only the DNS admin can publish a TLSA RR in a domain, and the admin already has the ability to get a cert for that domain, we feel that DANE validated certs have (approximately) the same level of trust.

Almost the end!

- DNSSEC was supposed to secure DNS and prevent spoofing / cache poisoning....
- But, it's actually a secure publishing method that enforces limits on the scope where a user can publish.
- This opens the door for all sorts of interesting and innovative applications.

For more information:

1. Come find me (or Ondřej Surý)
2. http://datatracker.ietf.org/wg/dane/charter/

FIN

Certificate.

```
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number:
          2f:df:bc:f6:ae:91:52:6d:0f:9a:a3:df:40:34:3e:9a
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte SGC CA
      Validity
          Not Before: Dec 18 00:00:00 2009 GMT
          Not After : Dec 18 23:59:59 2011 GMT
      Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=www.google.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e8:f9:86:0f:90:fa:86:d7:df:bd:72:26:b6:d7:
                    44:02:83:78:73:d9:02:28:ef:88:45:39:fb:10:e8:
                    7c:ae:a9:38:d5:75:c6:38:eb:0a:15:07:9b:83:e8:
                    [SNIP]
    Signature Algorithm: sha1WithRSAEncryption
        9f:43:cf:5b:c4:50:29:b1:bf:e2:b0:9a:ff:6a:21:1d:2d:12:
        c3:2c:4e:5a:f9:12:e2:ce:b9:82:52:2d:e7:1d:7e:1a:76:96:
```