NCSC conference, january 23, 2013
Marco Davids
Technical Advisor

DANE, the next big thing (after DNSSEC)

SIDN

SIDN

Foundation for Internet Domain Registration in the Netherlands (SIDN)

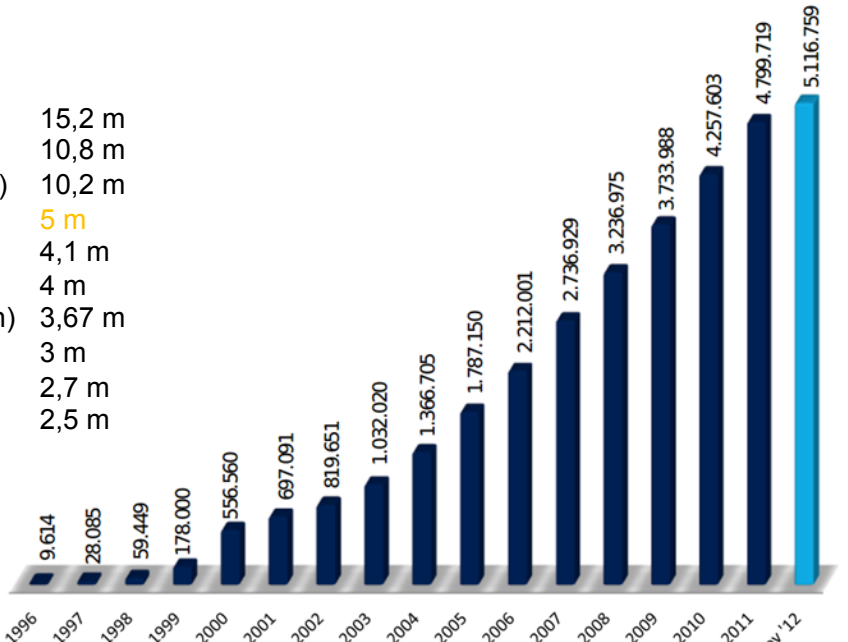
- Registry for .nl

.nl in figures

Top 10 ccTLD's

1 .DE (Germany)	15,2 m
2 .TK (Tokalau)	10,8 m
3 .UK (United kingdom)	10,2 m
4 .NL (Netherlands)	5 m
5. CN (PR of China)	4,1 m
6 .RU (Russian Fed.)	4 m
7 .EU (European Union)	3,67 m
8. BR (Brazil)	3 m
9. AR (Argentine)	2,7 m
10 .AU (Australia)	2,5 m

(source: CENTR, sept 2012)



(source: SIDN)

.nl today

- High domain density
- 1th TLD in terms of DNSSEC

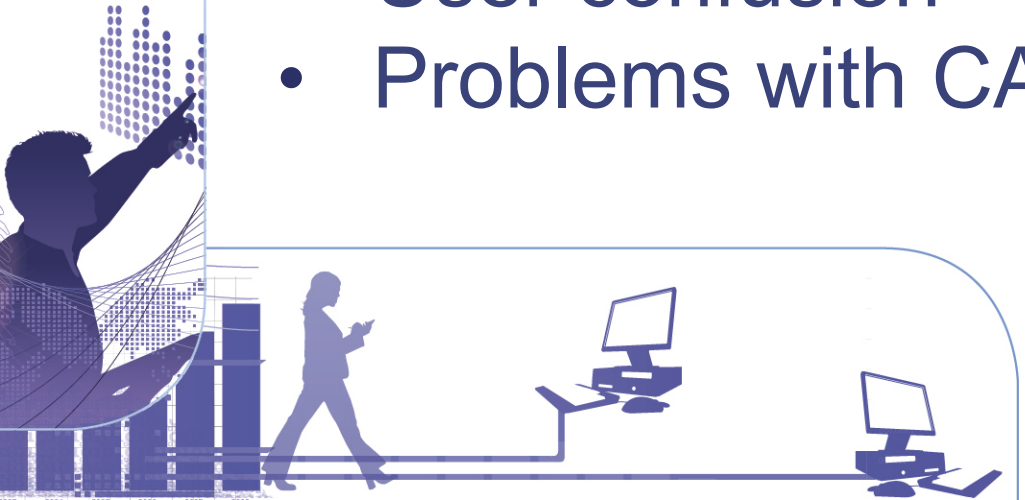
The problem

PKI system drawbacks:

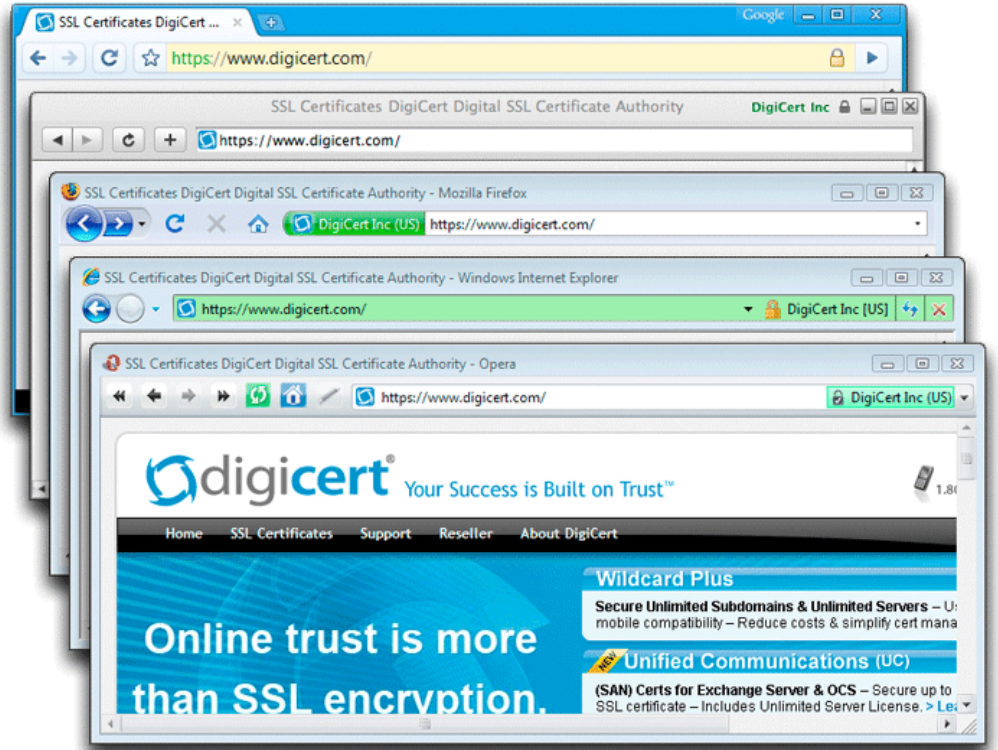
- Complex…
- Lack of quality…
- Architectural weaknesses…
- Implementation issues…
- But, more important (in this context)…

PKI system drawbacks

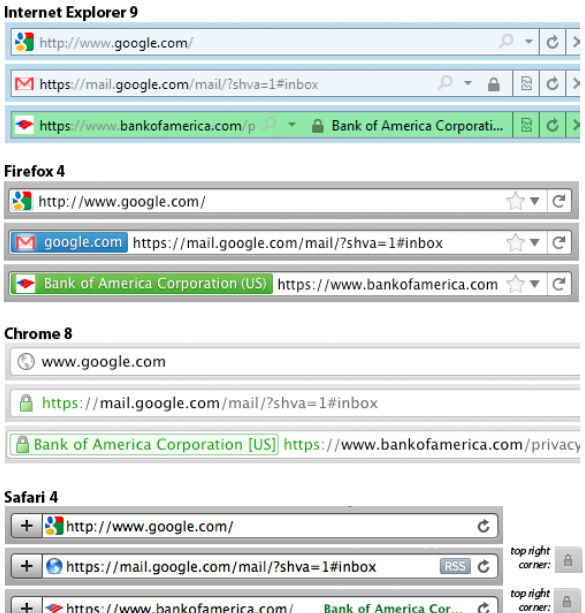
- User confusion
- Problems with CA's



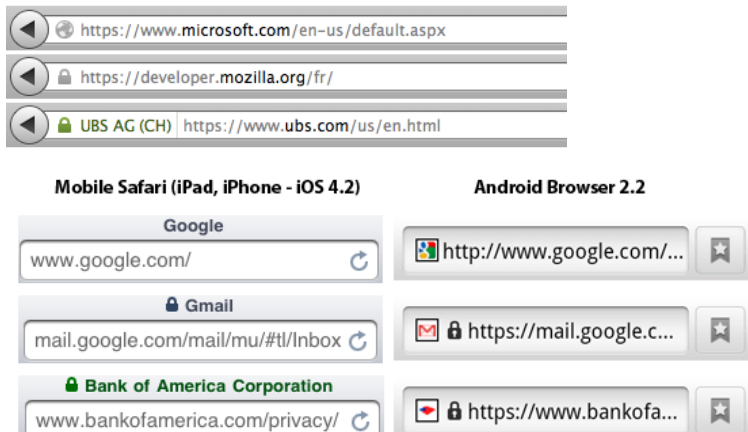
PKI: SSL/TLS


SSL Certificates DigiCert ...
https://www.digicert.com/
SSL Certificates DigiCert Digital SSL Certificate Authority
DigiCert Inc
https://www.digicert.com/
SSL Certificates DigiCert Digital SSL Certificate Authority - Mozilla Firefox
DigiCert Inc (US)
https://www.digicert.com/
SSL Certificates DigiCert Digital SSL Certificate Authority - Windows Internet Explorer
https://www.digicert.com/
DigiCert Inc [US]
SSL Certificates DigiCert Digital SSL Certificate Authority - Opera
https://www.digicert.com/
DigiCert Inc (US)
digicert
Your Success is Built on Trust™
Home
SSL Certificates
Support
Reseller
About DigiCert
Online trust is more than SSL encryption.
Wildcard Plus
Secure Unlimited Subdomains & Unlimited Servers – U
mobile compatibility – Reduce costs & simplify cert mana
NEW
Unified Communications (UC)
(SAN) Certs for Exchange Server & OCS – Secure up to
SSL certificate – Includes Unlimited Server License. > Le

Where do you pay attention to in your browser?



And what about your mobile device?



Many CA's…

A-Trust-nQual-03
Chambers of Commerce Root
Global Chambersign Root
Chambers of Commerce Root - 2008
Global Chambersign Root - 2008
Actalis Authentication Root CA
AddTrust Class 1 CA Root
AddTrust External CA Root
AddTrust Public CA Root
AddTrust Qualified CA Root
AffirmTrust Commercial
AffirmTrust Networking
AffirmTrust Premium
AffirmTrust Premium ECC
EC-ACC
America Online Root Certification Authority 1
America Online Root Certification Authority 2
Juur-SK
EE Certification Centre Root CA

20…

Many CA's…

Autoridad de Certificacion Firmaprofesional CIF A62634068
Autoridad de Certificacion Firmaprofesional CIF A62634068
Baltimore CyberTrust Root
Buypass Class 2 CA 1
Buypass Class 3 CA 1
Buypass Class 2 Root CA
Buypass Class 3 Root CA
Certinomis - Autorité Racine
Class 2 Primary CA
certSIGN ROOT CA
ePKI Root Certification Authority
CNNIC ROOT
COMODO ECC Certification Authority
AAA Certificate Services
Secure Certificate Services
Trusted Certificate Services
COMODO Certification Authority
ComSign Secured CA
ComSign CA
Cybertrust Global Root
Deutsche Telekom Root CA 2

40…

Many CA's…

S-TRUST Authentication and Encryption Root CA 2005:PNS
Certigna
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert High Assurance EV Root CA
[DISABLED] DigiNotar Root CA
DST ACES CA X6
Digital Signature Trust Co. Global CA 1
Digital Signature Trust Co. Global CA 3
DST Root CA X3
CA Disig
EBG Elektronik Sertifika Hizmet Sağlayıcısı
ACEDICOM Root
e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi
Entrust Root Certification Authority
Entrust.net Secure Server Certification Authority
Entrust.net Certification Authority (2048)
[DISABLED] Digisign Server ID - (Enrich)
Equifax Secure CA
Equifax Secure eBusiness CA 2
[DISABLED] MD5 Collisions Inc. (http://www.phreedom.org/md5)

60…

Many CA's…

Equifax Secure Global eBusiness CA-1
Equifax Secure eBusiness CA-1
Root CA Generalitat Valenciana
GeoTrust Global CA
GeoTrust Global CA 2
GeoTrust Universal CA
GeoTrust Universal CA 2
GeoTrust Primary Certification Authority
GeoTrust Primary Certification Authority - G2
GeoTrust Primary Certification Authority - G3
GlobalSign
GlobalSign Root CA
Go Daddy Root Certificate Authority - G2
Taiwan GRCA
GTE CyberTrust Global Root
Digisign Server ID (Enrich)
Hellenic Academic and Research Institutions RootCA 2011
Hongkong Post Root CA 1
Izenpe.com
SecureSign RootCA11

80…

Many CA's…

ApplicationCA - Japanese Government
Microsec e-Szigno Root CA
Microsec e-Szigno Root CA 2009
NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado
NetLock Kozjegyzoi (Class A) Tanusitvanykiado
NetLock Uzleti (Class B) Tanusitvanykiado
NetLock Expressz (Class C) Tanusitvanykiado
NetLock Arany (Class Gold) Főtanúsítvány
Network Solutions Certificate Authority
IGC/A
QuoVadis Root Certification Authority
QuoVadis Root CA 2
QuoVadis Root CA 3
RSA Security 2048 v3
Security Communication RootCA2
Security Communication EV RootCA1
Security Communication Root CA
SecureTrust CA
Secure Global CA
AC Raíz Certicámara S.A.

100…

Many CA's…

```
Sonera Class1 CA
Sonera Class2 CA
Staat der Nederlanden Root CA
Staat der Nederlanden Root CA - G2
Starfield Class 2 CA
Starfield Root Certificate Authority - G2
Starfield Services Root Certificate Authority - G2
StartCom Certification Authority
StartCom Certification Authority
StartCom Certification Authority G2
Swisscom Root CA 1
SwissSign Platinum CA - G2
SwissSign Gold CA - G2
SwissSign Silver CA - G2
T-TeleSec GlobalRoot Class 3
TWCA Root Certification Authority
TC TrustCenter Class 2 CA II
TC TrustCenter Class 3 CA II
TC TrustCenter Universal CA I
TC TrustCenter Universal CA III
TDC OCES CA
```

120…

Many CA's…

TDC Internet Root CA
Thawte Server CA
Thawte Premium Server CA
thawte Primary Root CA
thawte Primary Root CA - G2
thawte Primary Root CA - G3
Go Daddy Class 2 CA
UTN-USERFirst-Network Applications
UTN - DATACorp SGC
UTN-USERFirst-Client Authentication and Email
UTN-USERFirst-Hardware
UTN-USERFirst-Object
Trustis FPS Root CA
TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
Certum CA
Certum Trusted Network CA
http://www.valicert.com/

140…

Many CA's…

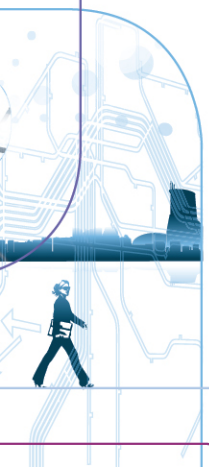
```
VeriSign Class 3 Public PCA - G5
VeriSign Class 3 Public PCA
VeriSign Class 1 Public PCA
VeriSign Class 1 Public PCA - G2
VeriSign Class 3 Public PCA - G4
VeriSign Class 2 Public PCA - G2
VeriSign Class 3 Public PCA - G2
VeriSign Class 1 Public PCA - G3
VeriSign Class 2 Public PCA - G3
VeriSign Class 3 Public PCA - G3
VeriSign Class 4 Public PCA - G3
VeriSign Universal Root Certification Authority
Visa eCommerce Root
Wells Fargo Root Certificate Authority
WellsSecure Public Root Certificate Authority
OISTE WISeKey Global Root GA CA
XRamp Global Certification Authority
```

160…

Source: http://www.mozilla.org/projects/security/certs/

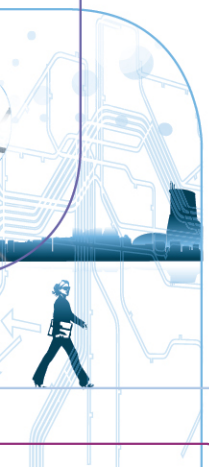
Bottom line:

- There are **many** CA's ('Certificate Authorities')…
- There ~~is risk of~~ are 'bad apples'
- No proper way of matching certificate with website
- No easy way to trust some CA's more than others
- Unclear for Mr. Joe Average



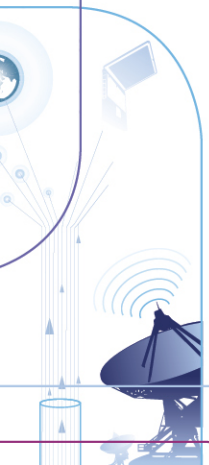
Solution?

- Certificate pinning
  - Not really scalable, but it saved Google's butt a number of times
- Notaries (like 'converge.io')
  - No uniform standard
  - Not very user-friendly



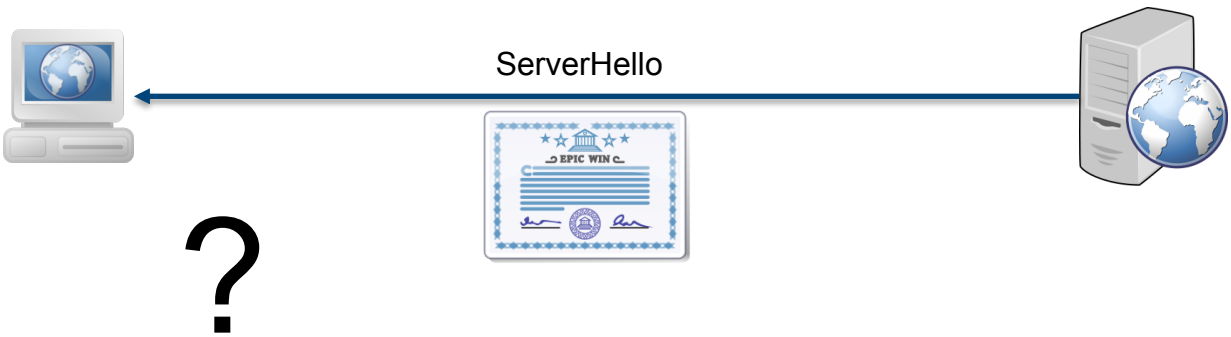
How DANE helps

The goal of DANE is to use the DNS (and DNSSEC) to provide clients with additional information about the cryptographic credentials associated with a domain



The problem in pictures!

Handshake

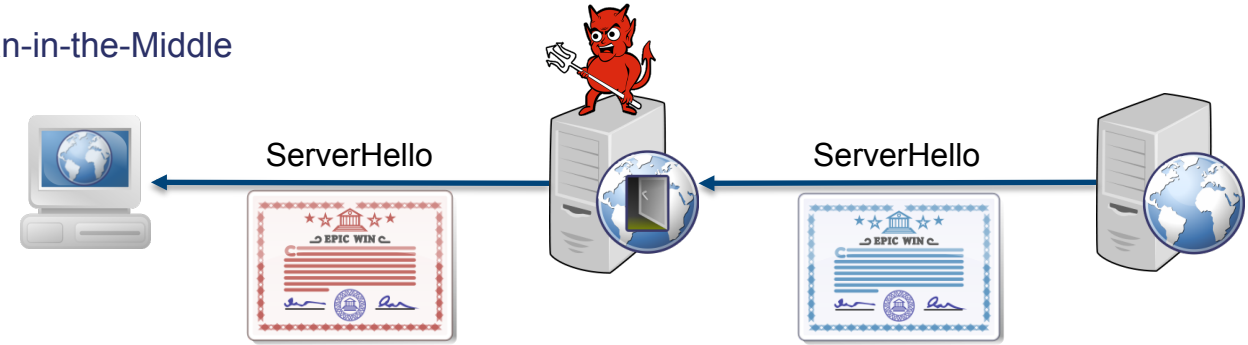


- Is the certificate valid? Yes/No
- If Yes: proceed with handshake
- If No, abort with a warning

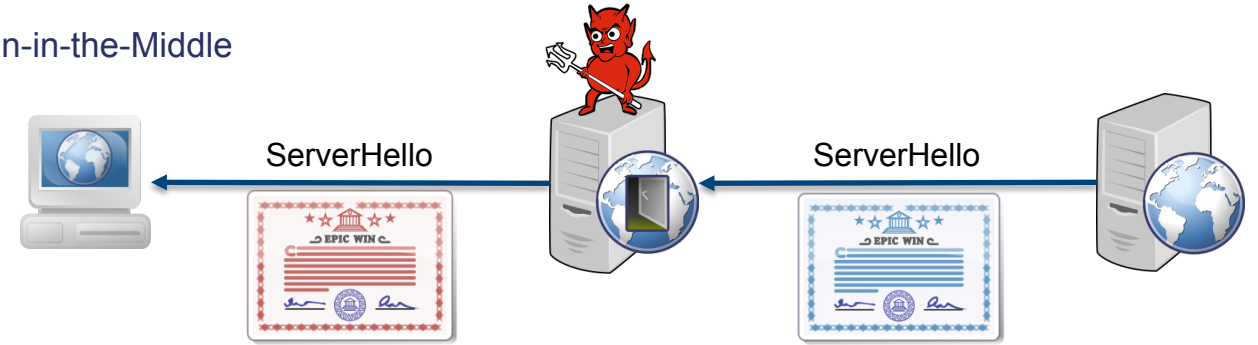
A valid certificate…

- Is not expired or revoked
- Validates with one of the many CA's
- Has a matching common name

Man-in-the-Middle



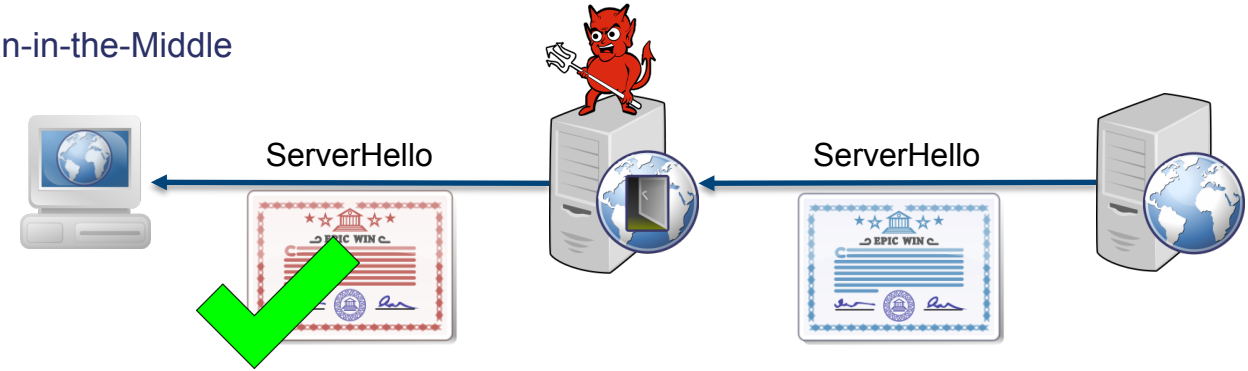
Man-in-the-Middle



The (fake) certificate is…

- Not expired or revoked
- Validates with one of the many CA's
- Has a matching common name

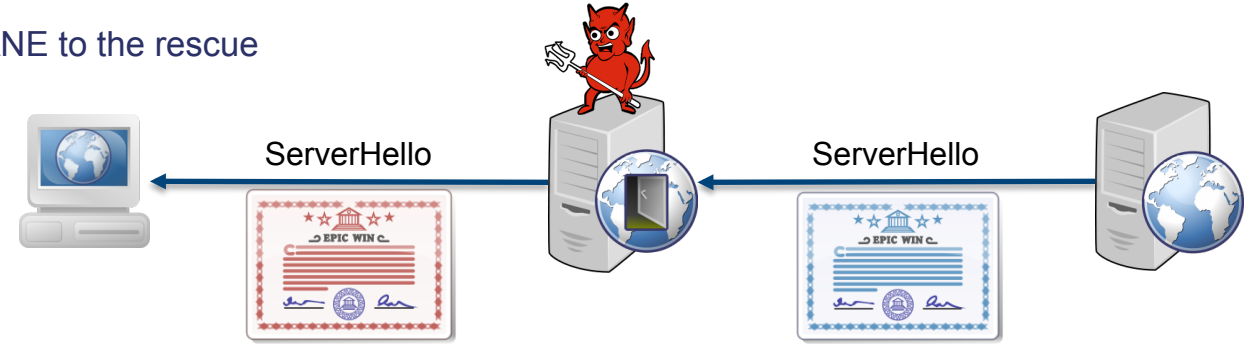
Man-in-the-Middle



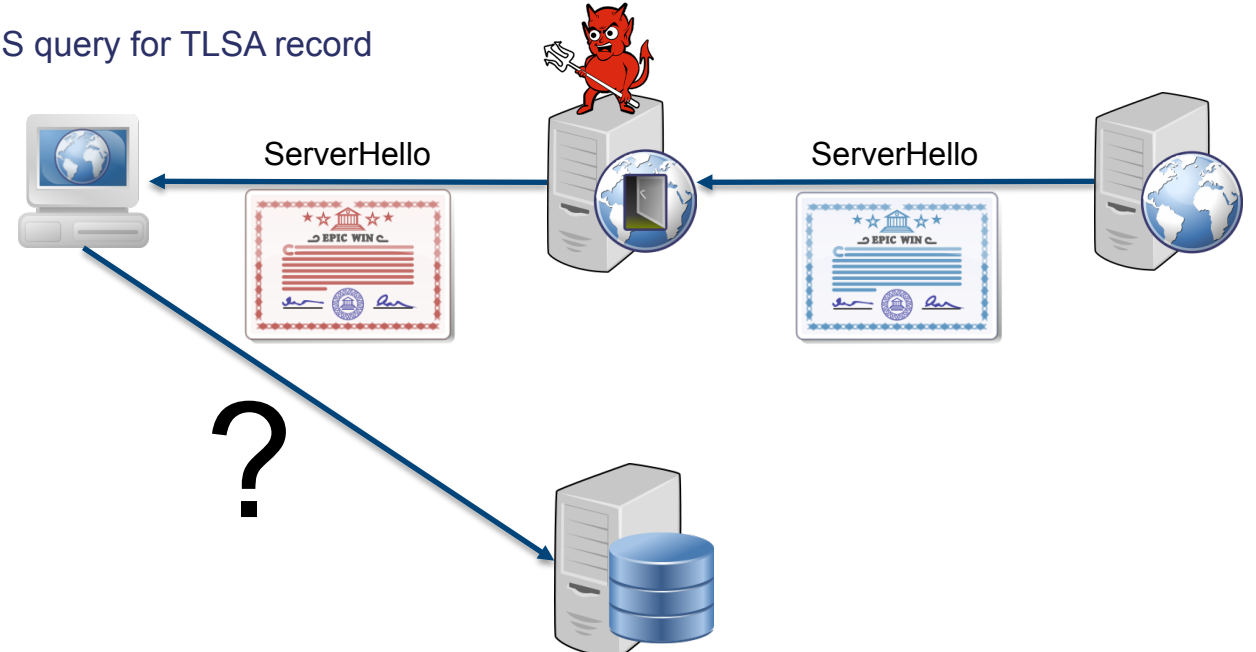
The (fake) certificate is…

- Not expired or revoked
- Validates with one of the many CA's
- Has a matching common name

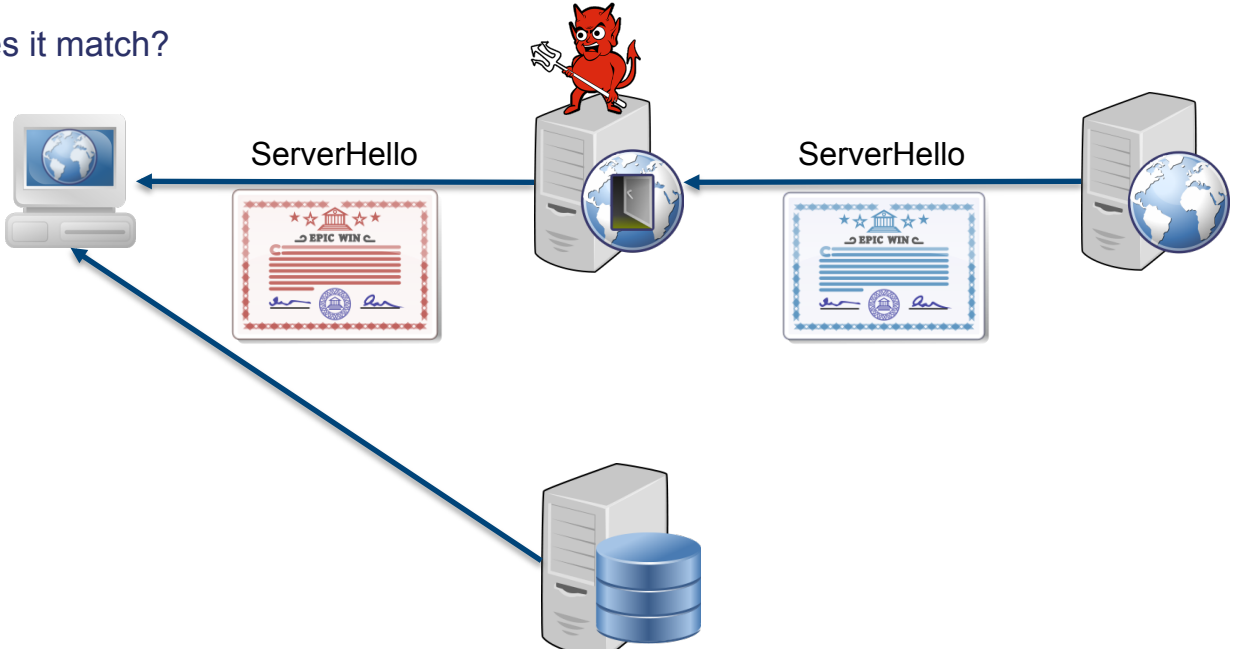
DANE to the rescue



DNS query for TLSA record



Does it match?




```
_443._tcp.www.example.nl. IN TLSA (
      1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```

Genuine certificate matches the TLSA, fake certificate does not

==

```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
           7983a1d16e8a410e4561cb106618e971 )
```

!=

```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
           7983a1d16e8a410e4561cb106618e971 )
```

Genuine certificate matches the TLSA, fake certificate does not

==

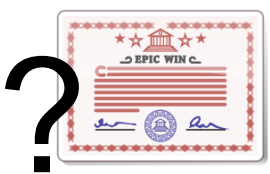
```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
           7983a1d16e8a410e4561cb106618e971 )
```

!=

```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
           7983a1d16e8a410e4561cb106618e971 )
```

Without DANE…


```
_443._tcp.www.example.nl. IN TLSA (
      1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```



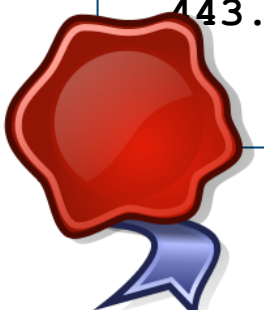

```
_443._tcp.www.example.nl. IN TLSA (
      1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```

Without DANE… both certificates would have been accepted


```
_443._tcp.www.example.nl. IN TLSA (
      1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```


```
_443._tcp.www.example.nl. IN TLSA (
      1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```

```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
           7983a1d16e8a410e4561cb106618e971 )
```



```
443._tcp.www.example.nl. IN TLSA (
    1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
          7983a1d16e8a410e4561cb106618e971 )
```

```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
           7983a1d16e8a410e4561cb106618e971 )
```

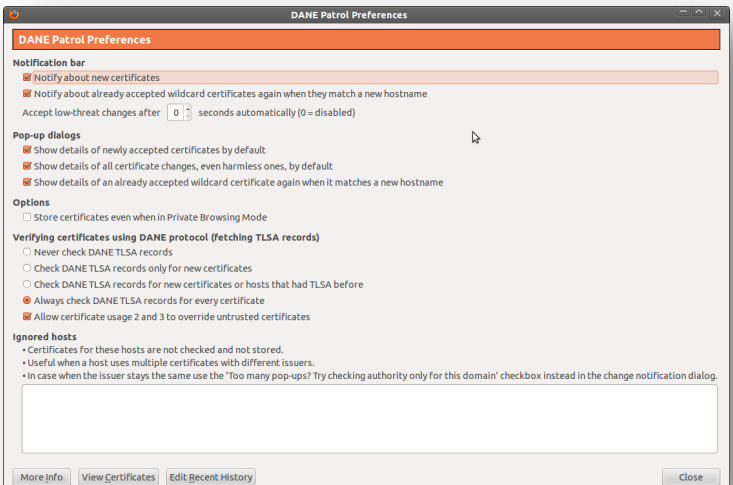
```
_443._tcp.www.example.nl.  IN RRSIG TLSA 8 5 300 (
   20130423112228 20130115102228 52044 example.nl.
   bnMyNbCO3MwRAvVmIX7KHpUGgIdpBFMz2ICMQ0gJz7UD
   A3tz0EKmBjqxOdwZaZNj2KrtxFJ2ta7elURYIHTpFF19
   +hJFTpeBJLKlJ636iLCyQCSXAYTLEiu7vOP2nnX8y6+M
   g+tOku4XNpk/HsolelmIA+Zxkj8Zxj+YxdedUlo= )
```

Current status

- IETF RFC6698 (august 2012)
- Early adopter stage
- Tools to generate TLSA records
- Support in BIND 9.9.1 and up
- Support in various other software

- No widespread use of it (yet)
- Mozilla / Google Chrome are ‘looking into it’ and experimenting
- Add-ons / extensions exist

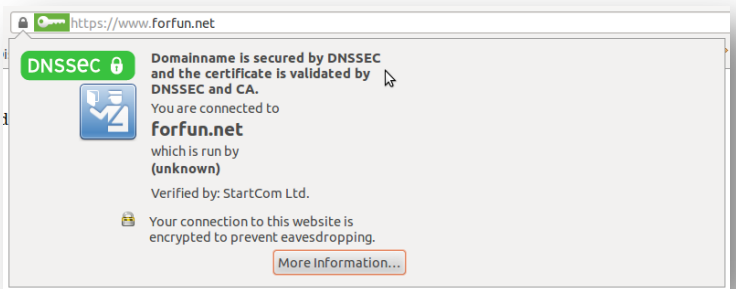
DANE standard



DANE patrol
By CZ.NIC labs
(fork of ‘Certificate Patrol’)

https://labs.nic.cz/page/1207/dane-patrol/

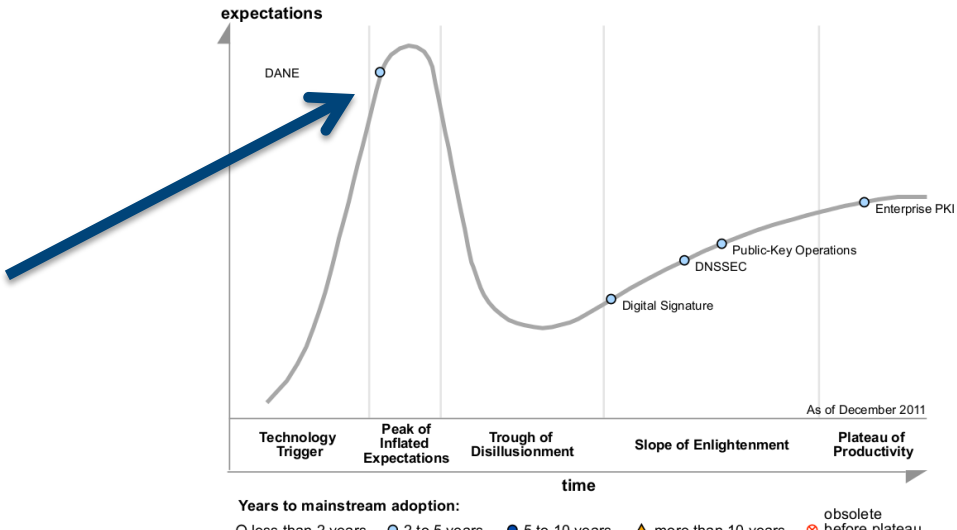
DANE standard



DNSSEC/TLSA validator
By Paul Wouters
(based on work done by CZ.NIC and D. Groenewegen)

http://people.redhat.com/pwouters/

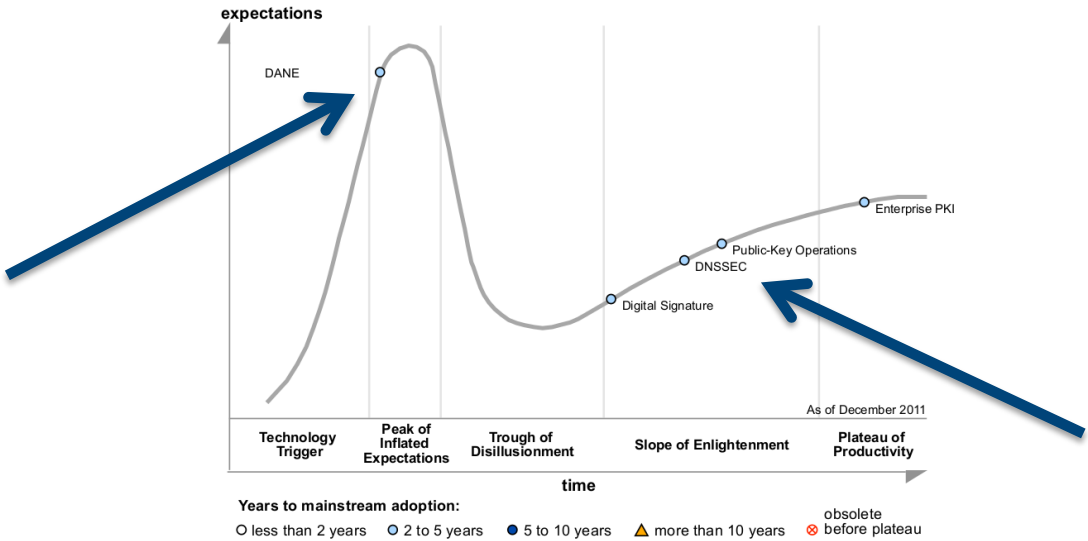
Hype cycle



This chart is a composite, derived from Gartner published Hype Cycles.
The particular combination and comparison of items made here has not been reviewed by Gartner.

by courtesy of: SURFnet

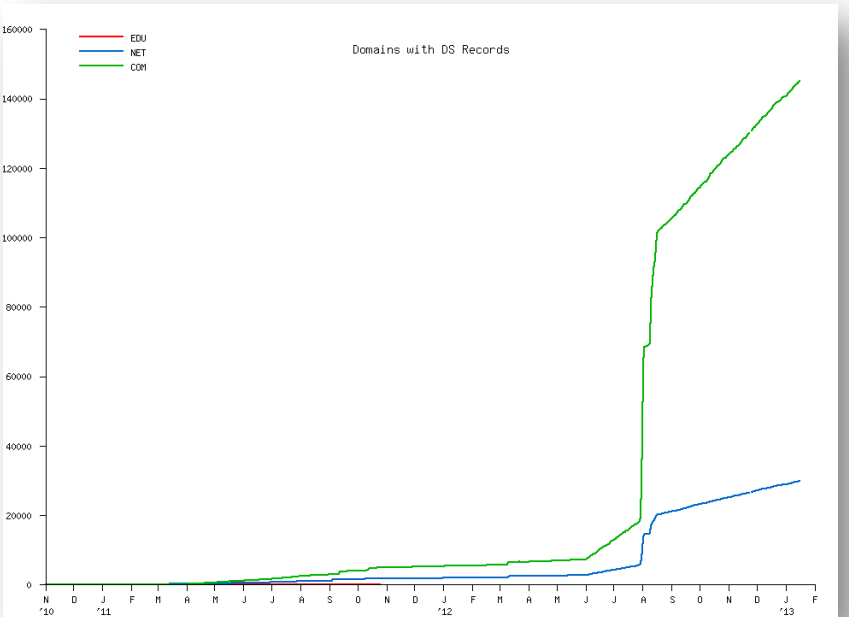
Hype cycle



This chart is a composite, derived from Gartner published Hype Cycles.
The particular combination and comparison of items made here has not been reviewed by Gartner.

by courtesy of: SURFnet

The state of DNSSEC

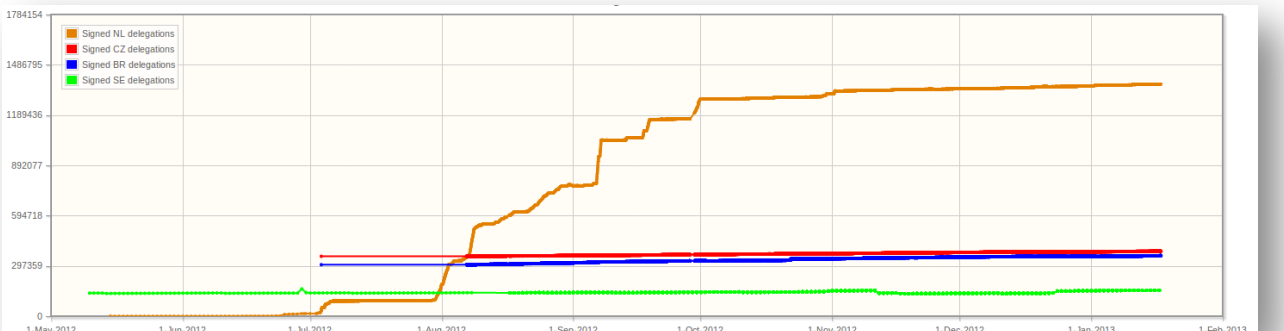


source: Verisign labs

Uptake of DNSSEC signed domains in .com, .net, .edu

.edu : 0.9%
.net : 0.2 %
.com: 0.15 %

The state of DNSSEC

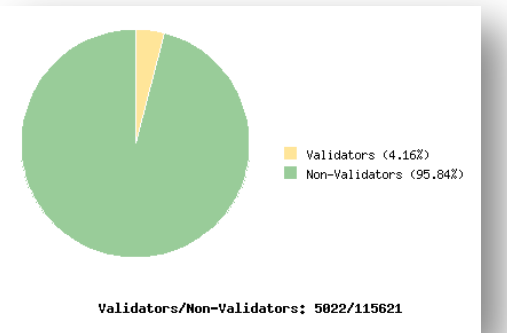


Uptake of DNSSEC signed domains in .nl, .cz, .br and .se

For .nl it is 26% !

source: PowerDNS

The state of DNSSEC validation



Worldwide ~4% DNSSEC validation

source: Verisign labs

The state of DNSSEC validation

Rank	# Resolvers	Avg Clients / Resolver	Weighted % of DNSSEC Resolution	Country
1	3	3	88.89%	Greenland
2	27	4	77.78%	Antigua and Barbuda
3	337	5	73.73%	Sweden
4	15	1	72.22%	Iran
5	8	30	63.22%	Libya
6	705	3	53.65%	Czech Republic
7	135	12	52.53%	Slovenia
8	11	9	52.04%	Equatorial Guinea
9	13350	9	48.57%	United States of America
10	177	6	47.08%	Finland

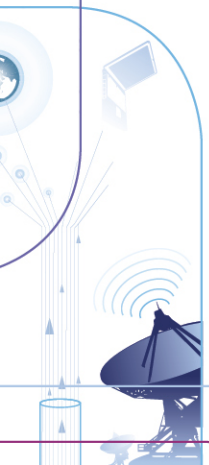
Some countries are doing really well

source: RIPE labs / Geoff Huston

Wrap up

Wrap up

- DANE adds additional layer of security to the PKI
- The standard is ratified by the IETF
- DANE is easy to implement, without much risk
- DNSSEC is required
- DNSSEC adoption is well on it's way
- Early adopters are already playing with it
- Browser-vendors are interested
- Things are looking good!



THANK YOU