VERISIGN®

DANE Demonstration

Duane Wessels, Verisign

ICANN 49 DNSSEC Workshop

March 26, 2014

VERISIGN

Outline

- What is DANE?
- The TLSA Record
- TLSA Browser Plugin
- Generating the TLSA Record
- Other uses for DANE

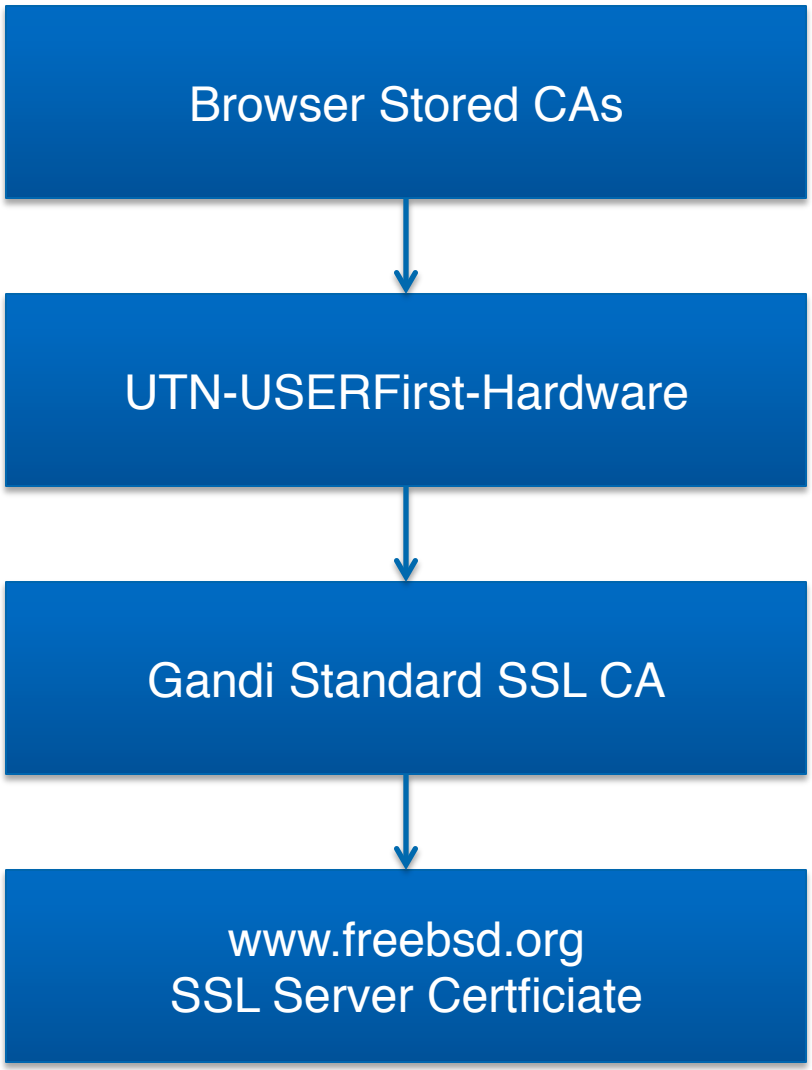
VERISIGN®

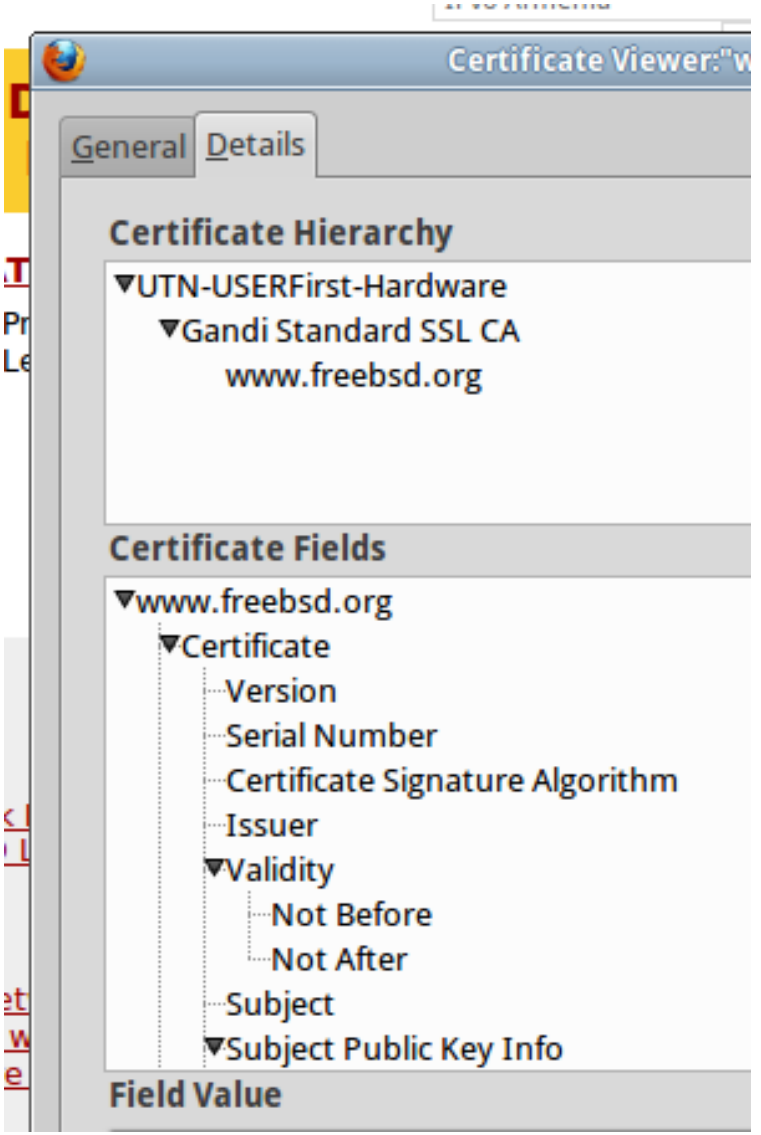
DNS-Based Authentication of Named Entities (DANE)

What is DANE?

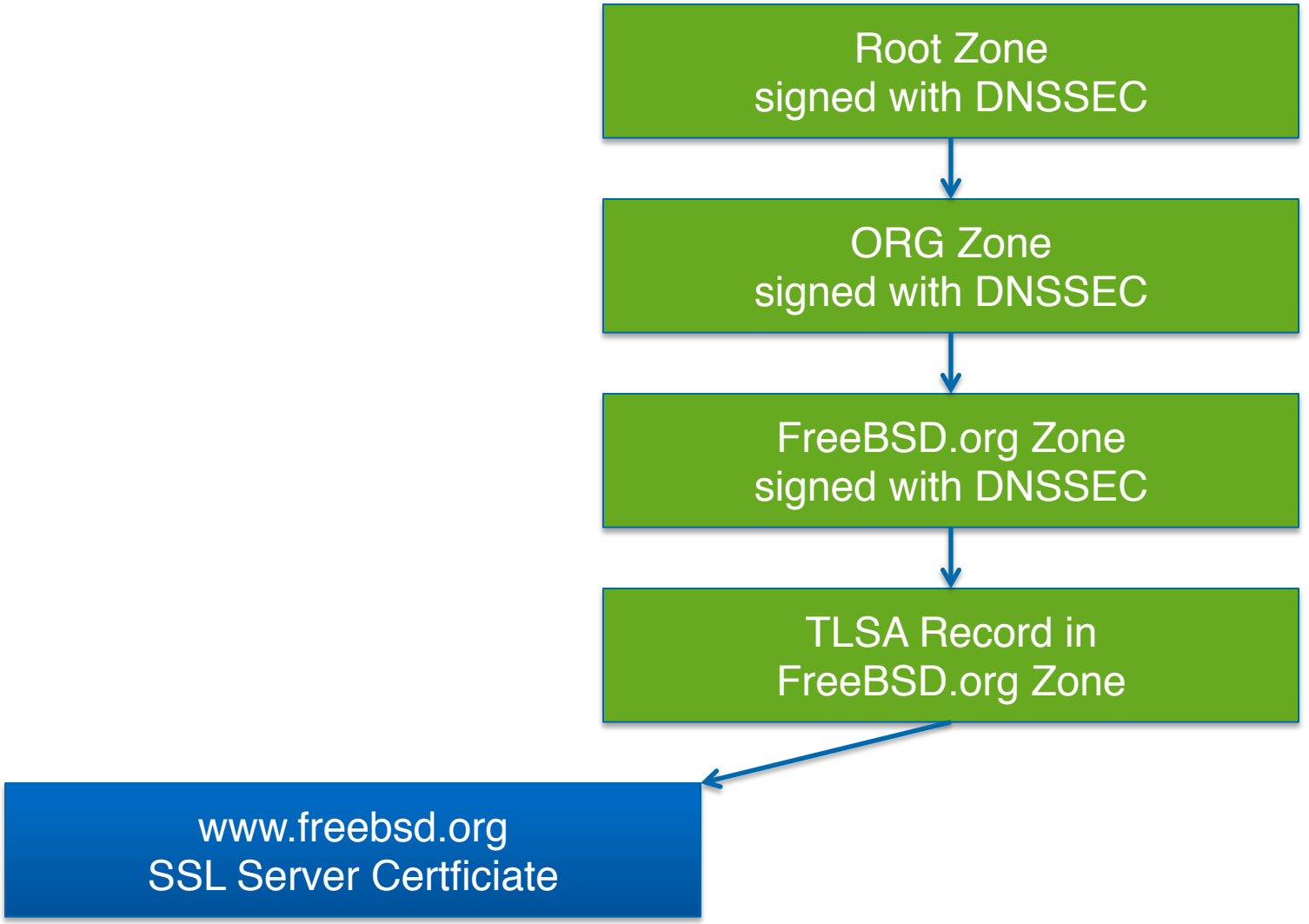
- A suite of RFCs describing how to represent and authenticate “named entities” in DNS and DNSSEC.
- Named Entities:
  - Web sites, and other servers
  - Email addresses
  - Jabber/Chat IDs
- RFC 6394 “Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)”
- RFC 6698 “The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA”
- Internet-Drafts: S/MIME, SMTP, IPSEC, PGP, OTR

The CA Way


Browser Stored CAs
UTN-USERFirst-Hardware
Gandi Standard SSL CA
www.freebsd.org
SSL Server Certficiate


Certificate Viewer:"w
General
Details
Certificate Hierarchy
UTN-USERFirst-Hardware
Gandi Standard SSL CA
www.freebsd.org
Certificate Fields
www.freebsd.org
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value

The DANE/TLSA Way



The DANE/TLSA Way

- TLSA can be used in other ways as we'll see next
  - Match only the public key part of a cert
  - Match a CA, rather than server cert
  - Specify new CA trust anchor

VERISIGN®

The TLSA Record

TLSA Record Names

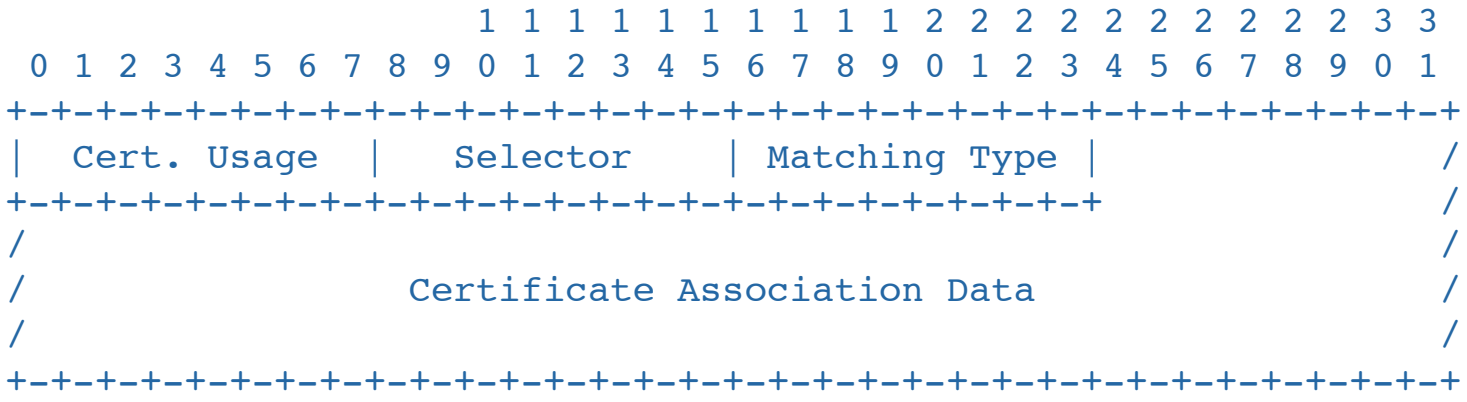
- Similar to SRV records
- Prefixed with port and protocol labels
- For example, the TLSA record for https://www.freebsd.org is at:

```
_443._tcp.www.freebsd.org.
```

- For SMTP submission, perhaps:

```
_587._tcp.mx1.freebsd.org.
```

TLSA Wire Data Format



TLSA Record Fields

- Certificate Usage
  - 0 = “CA constraint”
  - 1 = “service certificate constraint”
  - 2 = “trust anchor assertion”
  - 3 = “domain-issued certificate”
- Selector
  - 0 = full certificate
  - 1 = public key only
- Matching Type
  - 0 = exact match
  - 1 = match SHA-256 hash
  - 2 = match SHA-512 hash
- Certificate Association Data
  - full certificate, or public key data, or hash value

VERISIGN

Certificate Usage 0 – “CA constraint”

- The server’s cert must be validated by the CA cert referenced in the TLSA record.
- The CA cert must be part of the client’s normal set of trusted authorities.
- Any valid cert from the CA will be accepted.
  - But not other CAs known to the application.
  - Can get a new cert from same CA without updating TLSA record.

VERISIGN

Certificate Usage 1 – “service certificate constraint”

- The server’s cert must match the cert referenced in the TLSA record.
- The cert must validate via the application’s standard PKIX mechanisms.
- Must update TLSA record each time server’s cert changes.

Certificate Usage 2 – “trust anchor assertion”

- Specifies a new trust anchor for validating the server’s cert.
- Similar to usage 1, except the trust anchor need not be previously known to the application.

Certificate Usage 3 – “domain-issued certificate”

- Server’s cert must match the TLSA record.
- No other CA/PKIX validation necessary.

Size of Certificate Association Data

- SHA256 – 32 octets
- SHA512 – 64 octets
- Public (e.g. RSA) key – varies
  - 1024 bits – 128 octets
  - 2048 bits – 256 octets
  - 4096 bits – 512 octets
- Full certificate – varies
  - 4096 bit RSA key – approx 1400 octets

VERISIGN

For Today…

- Certificate Usage = 3 (domain-issued)
- Selector = 0 (full certificate)
- Matching Type = 1 (SHA256 hash)

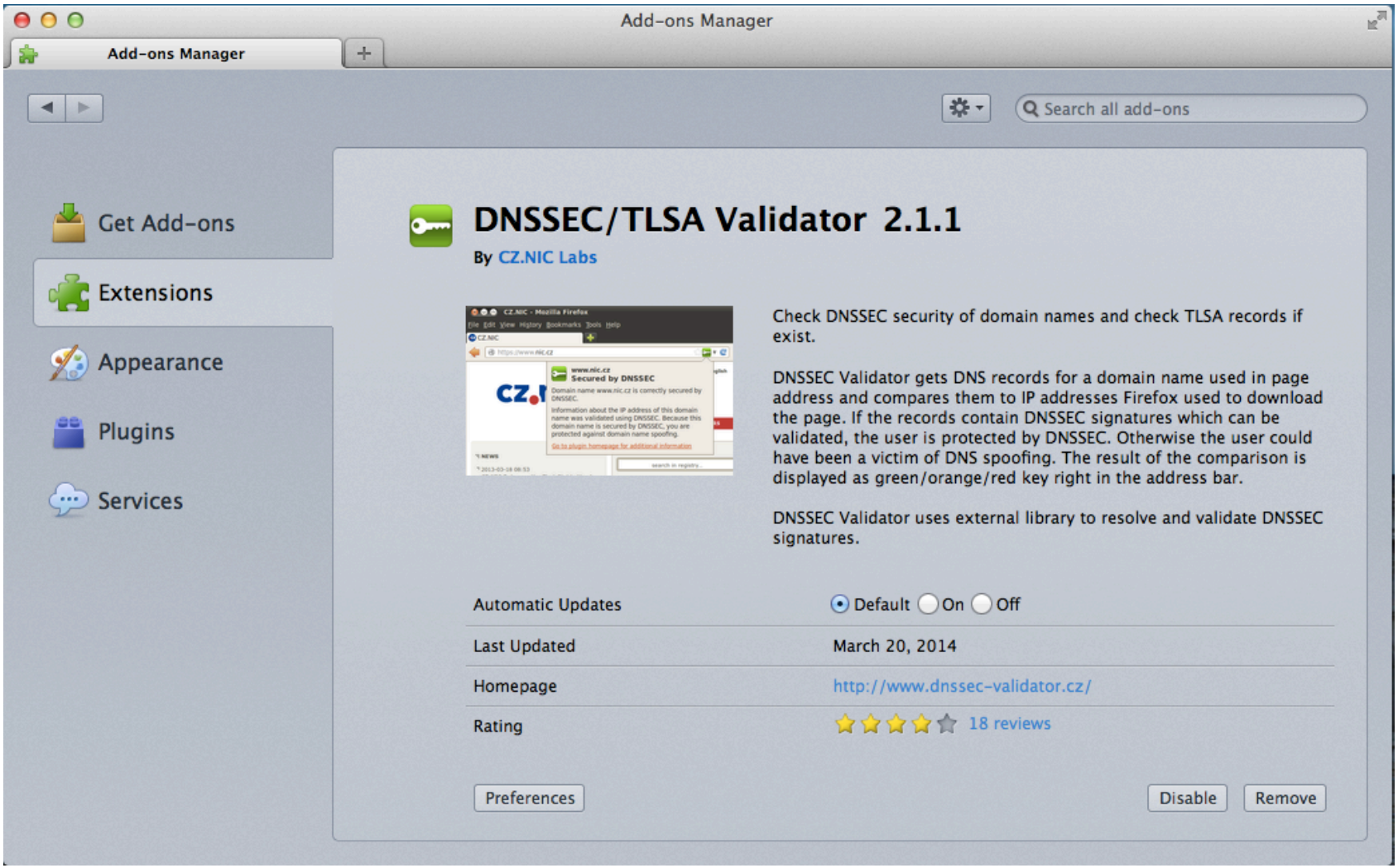
VERISIGN®

TLSA Browser Plugin

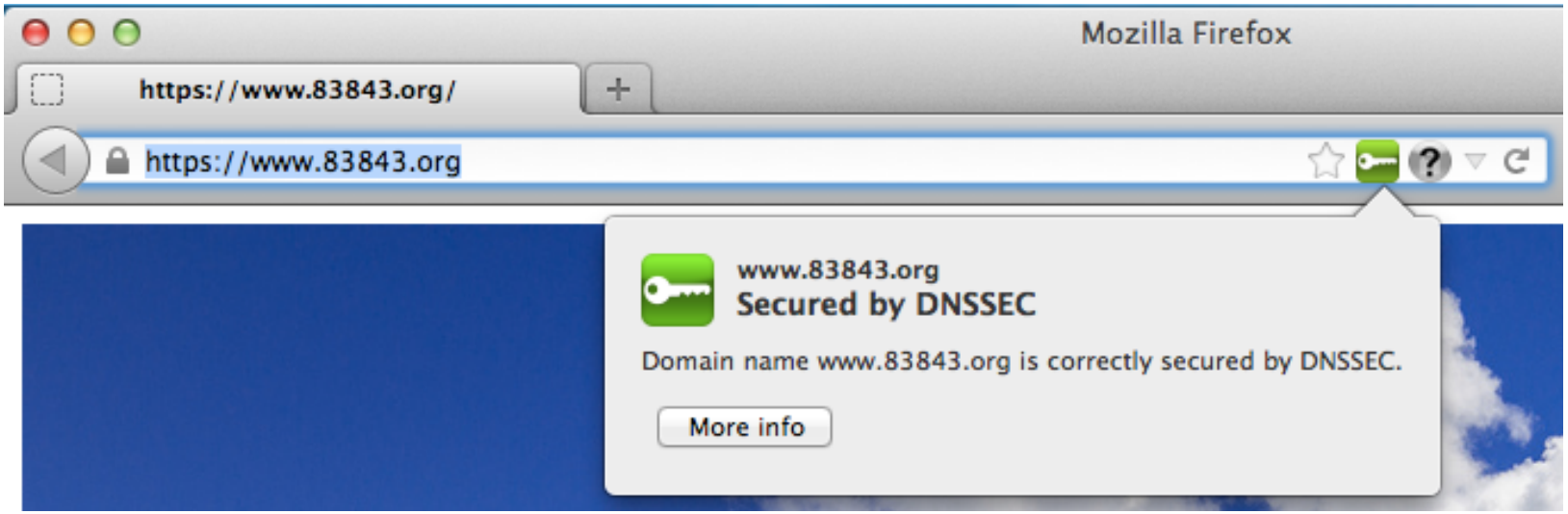
CZ.NIC's DNSSEC/TLSA Validator add-on for Web Browsers

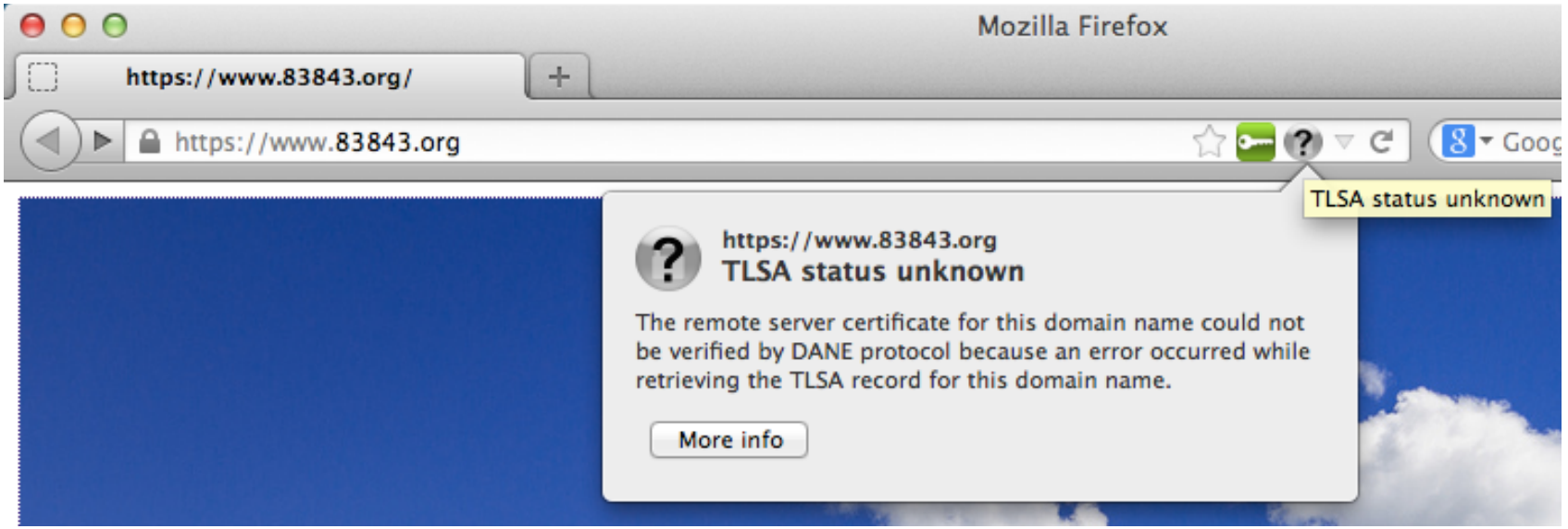
- https://www.dnssec-validator.cz/
- Indicates DNSSEC status
- Indicates TLSA status
- Works with:
  - Internet Explorer
  - Mozilla Firefox
  - Google Chrome
  - Opera
  - Apple Safari

Add-on Setup Screen



Zone is signed, but no TLSA record yet





VERISIGN®

Generating the TLSA Record

VERISIGN

First we need the certificate…

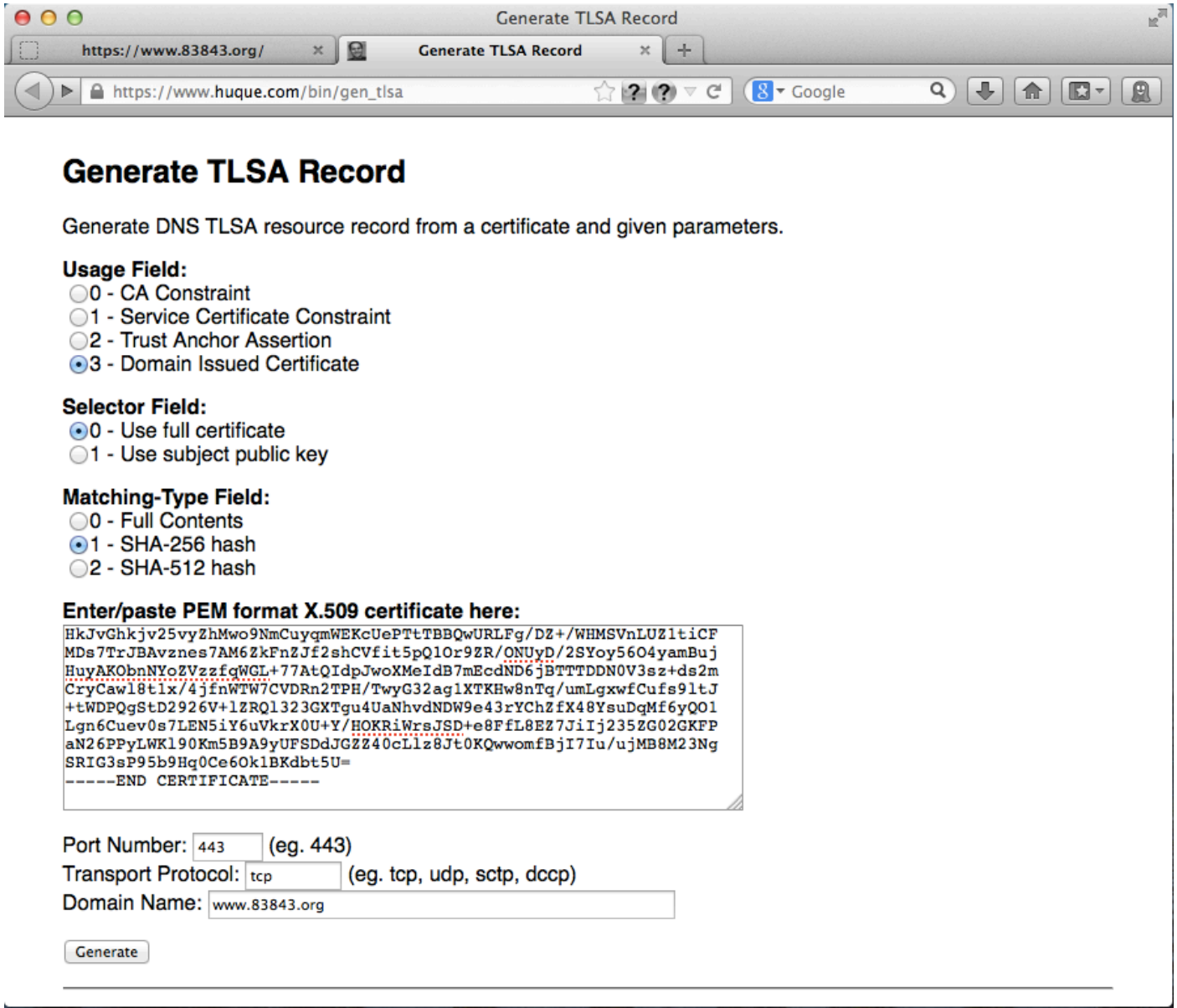
```
$ cat /etc/apache2/ssl/www.83843.org.crt
-----BEGIN CERTIFICATE-----
MIIEYDCCAkgCARcwDQYJKoZIhvcNAQEFBQAwgZgxCzAJBgNVBAYTAlVTMQswCQYD
VQQIEwJJRDEPMA0GA1UEBxMGTW9zY293MRcwFQYDVQQKEw5QYWNrZXQgUHVzaGVy
czELMAkGA1UECxMCQ0ExGjAYBgNVBAMTEVBhY2tldCBQdXNoZXJzIENBMSkwJwYJ
KoZIhvcNAQkBFhp3ZXNzZWxzQHBhY2tldC1wdXNoZXJzLmNvbTAeFw0xNDAzMjEx
NjQ4MzBaFw0yMzEyMTkxNjQ4MzBaMFMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJJ
RDEPMA0GA1UEBxMGTW9zY293MQ4wDAYDVQQKEwU4Mzg0MzEWMBQGA1UEAxMNd3d3
LjgzODQzLm9yZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ7GES+C
ROT0cbylBSpp+29iBunyD286/B6REv4aZvMq/l4a1vMwTi+OxZsjkc1IO0ghgWgr
V1gIMe65LtPo5qlqUp+MF/MdOn0BYRYKcDfYWhHh8+Ng5YZJ0GnZcZQdZB37OO5l
7tJhF9NB38wKlpm/z7zVSt1Eil2GE+0DfY2ME5wzkglK7a7dzSdMICyKqukCZF5z
KkE6MZrQKrKRUn8UfQ8gUizyZK2tkrcd4FjfG7z38vRnStc7OWvDMET1XzBWN1n/
u0y5zmOaGsyke4klobDYK910XvJn8gJ2kAUPtx14ktpRie0nJcJ5nxD3kFPKI6q8
wqC+Cu5rP6PZrMMCAwEAATANBgkqhkiG9w0BAQUFAAOCAgEAAh3/5zkdwjbf0+rr
Sb+b+IOZxoxTBNE49wwCYg++DZpKJOvrz0JWE0cJVpiqy1uwmMcntlGekf9pF2Yl
shOoFBo00lVQ9JGyT0q1uju8O9p5qpw+wM5gytemnSSgO1/Acy+AezTz8VqduHlx
ne+uzVQNeDa60ezQENjKSzJdTOGFYy10a8e/xznlGXVdRUbHDHXHErIcYQgd8aDv
HkJvGhkjv25vyZhMwo9NmCuyqmWEKcUePTtTBBQwURLFg/DZ+/WHMSVnLUZ1tiCF
MDs7TrJBAvznes7AM6ZkFnZJf2shCVfit5pQ1Or9ZR/ONUyD/2SYoy56O4yamBuj
HuyAKObnNYoZVzzfqWGL+77AtQIdpJwoXMeIdB7mEcdND6jBTTTDDN0V3sz+ds2m
CryCawl8t1x/4jfnWTW7CVDRn2TPH/TwyG32ag1XTKHw8nTq/umLgxwfCufs9ltJ
+tWDPQgStD2926V+lZRQl323GXTgu4UaNhvdNDW9e43rYChZfX48YsuDqMf6yQO1
Lgn6Cuev0s7LEN5iY6uVkrX0U+Y/HOKRiWrsJSD+e8FfL8EZ7JiIj235ZG02GKFP
aN26PPyLWKl90Km5B9A9yUFSDdJGZZ40cLlz8Jt0KQwwomfBjI7Iu/ujMB8M23Ng
SRIG3sP95b9Hq0Ce6Ok1BKdbt5U=
-----END CERTIFICATE-----
```

VERISIGN

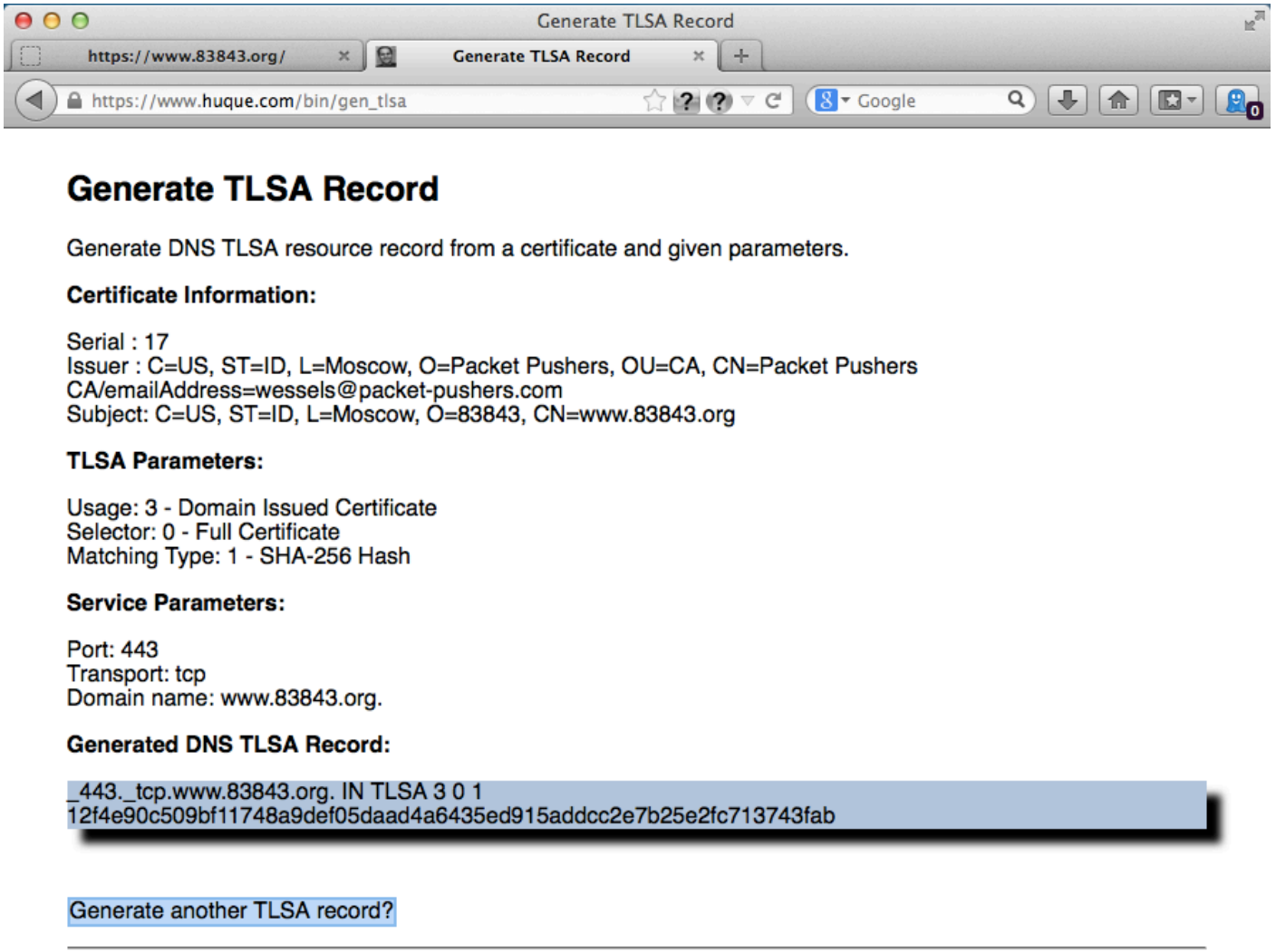
Tools to Generate TLSA Records

- http://lmgtfy.com/?q=generate+tlsa
- https://www.huque.com/bin/gen_tlsa
- http://people.redhat.com/pwouters/hash-slinger/
- https://github.com/shuque/tlsa_rdata

Input to Shumon's TLSA Generator



Output from Shumon's TLSA Generator



Add TLSA Record to Zone

- Edit zone file, etc
- Wait an appropriate amount of time for cache expiry
- Check it with dig

```
; <<>> DiG 9.9.5 <<>> +norec @173.230.152.222 _443._tcp.www.83843.org tlsa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11434
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_443._tcp.www.83843.org.     IN        TLSA

;; ANSWER SECTION:
_443._tcp.www.83843.org. 15   IN        TLSA      3 0 1
12F4E90C509BF11748A9DEF05DAAD4A6435ED915ADDCC2E7B25E2FC7 13743FAB
```

Check Browser and Add-on

Other Uses for DANE/TLSA

VERISIGN

Postfix (SMTP)

- Postfix now looks for TLSA records
- http://www.postfix.org/TLS_README.html#client_tls_dane

VERISIGN

S/MIME

- draft-ietf-dane-smime
- New SMIMEA record type
- Records are named with hash of user part of email address:

```
3f51f4663b2b798560c5b9e16d6069a28727f62518c3a1b33f7f
5214._smimecert.example.com
```

VERISIGN

OpenPGP Keys

- draft-wouters-dane-openpgp-02
- New OPENPGPKEY record type
- openpgpkey-milter
  - “attempt to automatically PGP encrypt plaintext emails received by the MTA/MUA before relaying the message further towards the recipient(s).”

VERISIGN

Off-the-Record Messaging Protocol

- draft-wouters-dane-otrfp-01
- New OTRFP record type

Thank You

VERISIGN®