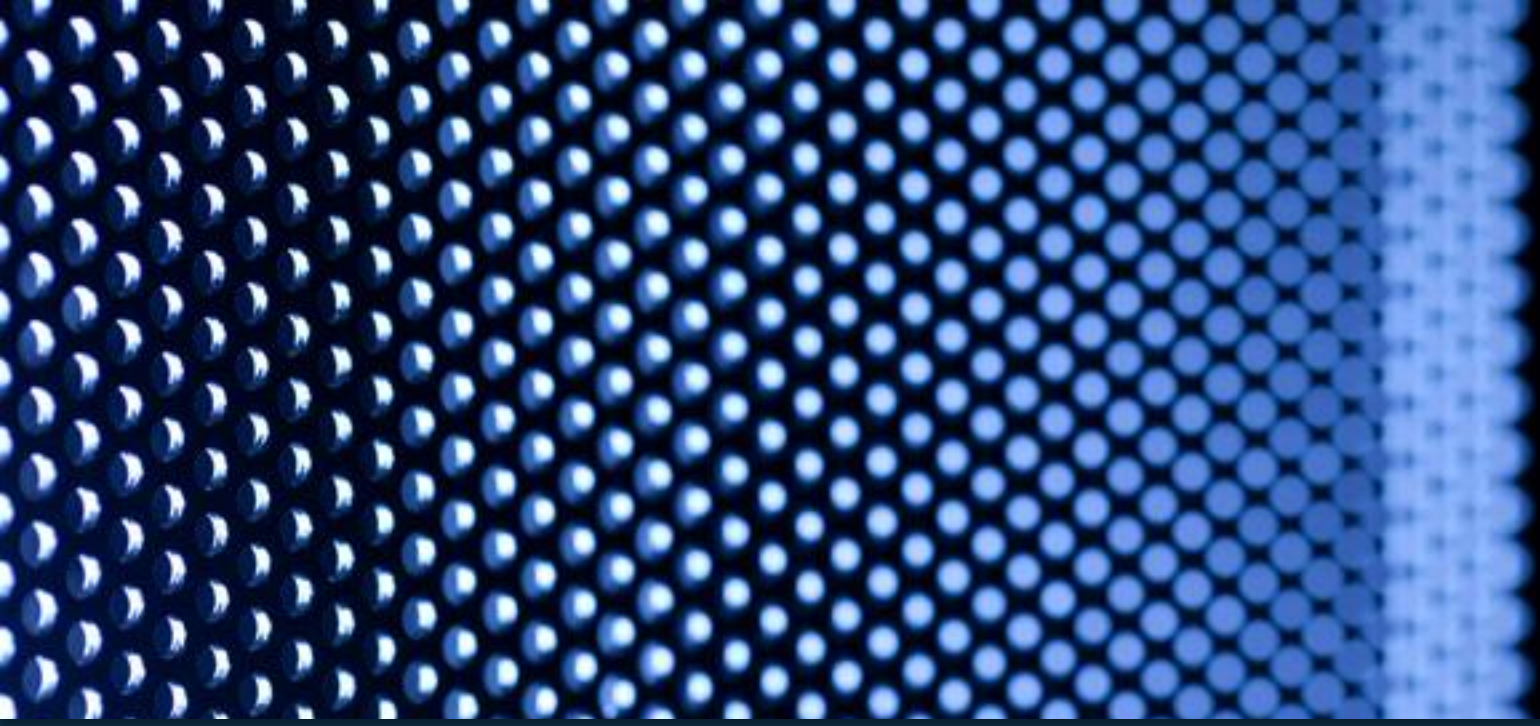


VERISIGN

Next Steps in DANE Adoption

Shumon Huque, Verisign Labs

DNS-OARC 2015 Fall Workshop, Montreal, Canada

October 3rd 2015

DNSSEC Deployment Overview

(a necessary precondition for DANE)

Brief DNSSEC Deployment Status

- DNS Root was signed in July 2010

- Top Level Domains: many are signed [1]:
  - All TLDs: 906 of 1,070 (84.7%), as of September 29th 2015
  - ccTLDs: 130 of 288 (45.1%)
  - New gTLDs: all are signed, 759 of 759 (100%)

- Reverse trees (in-addr.arpa and ip6.arpa) and the RIR level delegated zones are signed.

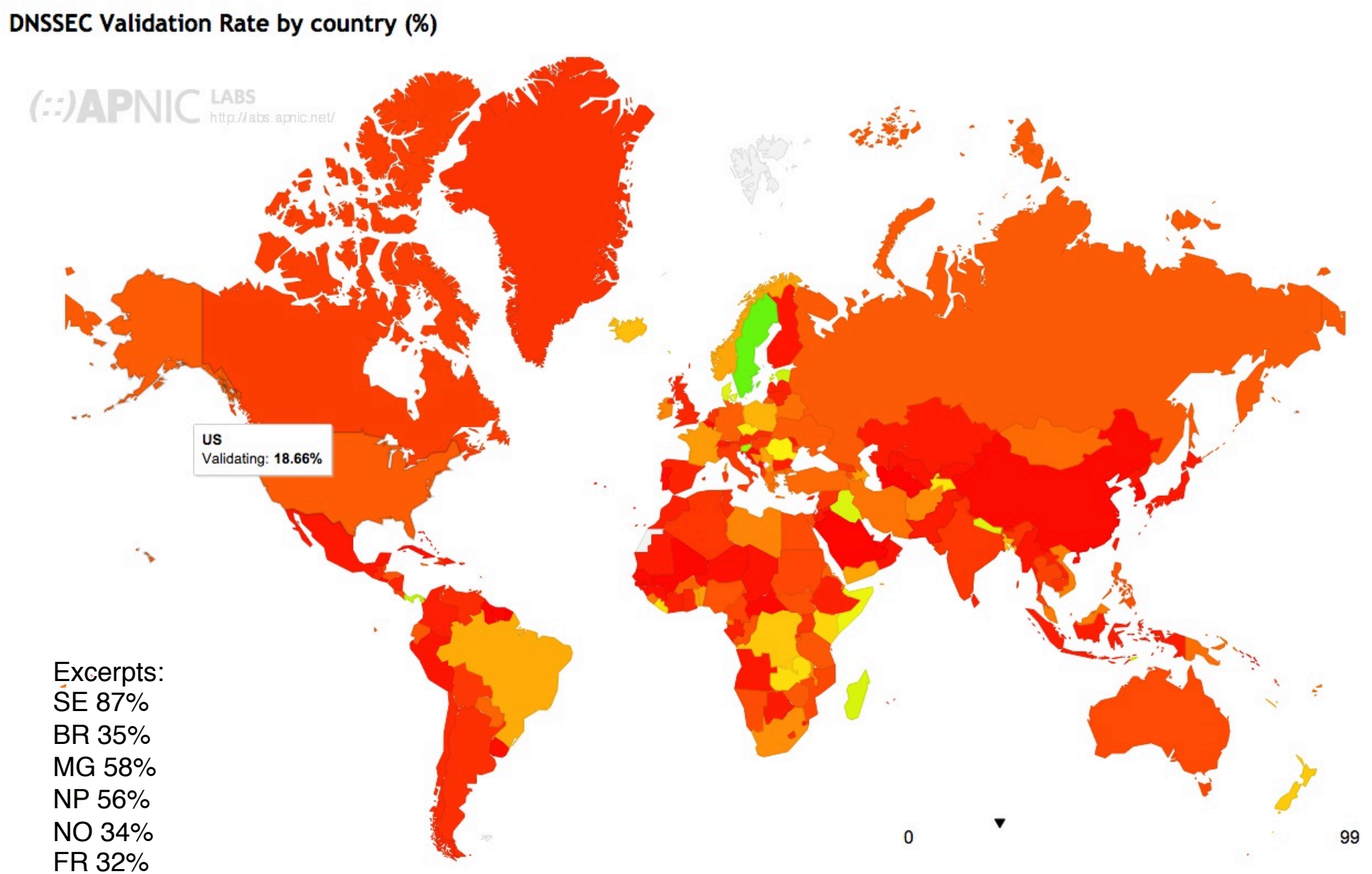
[1] https://www.huque.com/app/dnsstat

Use of DNSSEC Validation by Resolvers

- Some very large DNS resolver services are doing DNSSEC validation:
  - Google Public DNS (free; very widely used).
  - Comcast DNS [1]: ~ 18.1 million subscriber homes.
- US Gov FISMA IT security policy DNSSEC validation mandate (Spring 2014).
- Worldwide there is substantial amount of validation enabled queries, as measured by APNIC:
  - Roughly 15% of DNS queries by resolvers in the US perform DNSSEC validation.

[1] http://la51.icann.org/en/schedule/wed-dnssec/presentation-dnssec-dns-15oct14-en

stats.labs.apnic.net/dnssec



Excerpts:
SE 87%
BR 35%
MG 58%
NP 56%
NO 34%
FR 32%

These stats are a bit misleading …

- For DNSSEC to actually be useful, we need zones below the TLDs (*where applications and endpoints actually live*) to be signed!
- And the deployment numbers here are very small.

Deployment below the TLDs is woefully small

- Top Alexa sites (Sep 13 2015) ~ 1% deployment numbers:
  - Alexa top 100: Only 1 (paypal.com)
  - Alexa top 1,000: Only 10
  - Alexa top 10,000: Only 107
  - Alexa top 100,000: Only 1039

- Some very large gTLDs (< 1% penetration):
  - COM: 0.44% (518K of 118.4 million)
  - NET: 0.63% (94K of 14.9 million)
  - ORG: 0.51% (53K of 10.6 million)

Some brighter spots

- There are a few standout TLDs with substantial deployment but those are largely exceptions:
  - .NL (Netherlands) has over 2 million (40%) signed delegations [1]
  - .BR (Brazil) has ~ 700,000 signed delegations (20%) [2]

- US Federal government – FISMA OMB Mandate:
  - US .GOV federal: ~ 82% [3](Oct 2014)

[1] https://stats.sidnlabs.nl/
[2] https://twitter.com/_rubensk/status/570020637344837632?lang=en
[3] http://la51.icann.org/en/schedule/wed-dnssec/presentation-dnssec-deployment-gov-15oct14-en

DANE TLSA Record Deployment

TLSA Deployment Studies

- “Measuring DANE TLSA Deployment – Zhu, Wessels, Mankin, Heidemann”, IEEE Traffic Monitoring & Analysis workshop, April 2015.
- Zones under COM and NET Top Level Domains.
- TLSA records for the following services:
  - HTTPS (443), SMTP (25, 465, 587), XMPP (5222, 5269)
- Tiny number, but slow growth over time
- As of April 2015, 1533 TLSA names in 565 zones, in a scan of 541K signed zones.

A more recent TLSA scan

- COM and NET zones.
- Alexa Top 100 Thousand sites.

DNSSEC and TLSA Deployment

Source	#Zones	#Signed	%Signed	#TLSA zones	%TLSA of signed
COM	118m	524k	0.44%	4100	0.78%
NET	15m	94k	0.63%	1432	1.52%
Alexa 100k	~100k	1039	1.04%	44	4.23%

#TLSA zones: #signed zones that have deployed at least 1 TLSA record.
%TLSA of signed: What percentage of the signed zones are they.

Source	#TLSA records	#TLSA RRsets
COM	6,340	5,516
NET	2,583	2,279
Alexa 100k	120	118

Comparing COM+NET with previous study:

7795 TLSA names vs 1533
5532 zones vs 565

TLSA Application Service Types

Application service breakdown across all “RR sets”:

Source	SMTP	HTTP	XMPP
COM	4954 (89.8%)	467 (8.5%)	95 (1.7%)
NET	1832 (80.4%)	327 (14.4%)	120 (5.3%)
Alexa 100k	65 (55.1%)	49 (41.5%)	4 (3.4%)

Application service breakdown across all “TLSA Zones”:

Source	SMTP	HTTP	XMPP
COM	3969 (92.0%)	301 (7.0%)	45 (1.0%)
NET	1332 (82.9%)	222 (13.8%)	53 (3.3%)
Alexa 100k	33 (50.0%)	31 (47.0%)	2 (3.0%)

TLSA Parameters: Certificate Usage

Source	Usage Mode	Count	%
COM/NET	0: PKIX-TA	15	0.2%
	1: PKIX-EE	267	3.0%
	2: DANE-TA	163	1.8%
	3: DANE-EE	8568	95.1%
Alexa 100k	0: PKIX-TA	2	1.7%
	1: PKIX-EE	11	9.2%
	2: DANE-TA	0	0.0%
	3: DANE-EE	107	89.2%

DANE-EE dominant, followed by PKIX-EE.

(across all observed TLSA records)

TLSA Parameters: Selector

Source	Selector	Count	%
COM/NET	0: Cert	2705	30.0%
	1: SPKI	6308	70.0%
Alexa 100k	0: Cert	61	50.8%
	1: SPKI	59	49.2%

(across all observed TLSA records)

TLSA Parameters: Matching Type

Source	MatchingType	Count	%
COM/NET	0: Full	1	0.0%
	1: SHA256	7580	84.1%
	2: SHA512	1432	15.9%
Alexa 100k	0: Full	0	0.0%
	1: SHA256	120	100.0%
	2: SHA512	0	0.0%

SHA256 dominant.

(across all observed TLSA records)

Top SMTP DANE Sites

Numbers courtesy of Viktor Dukhovni.

24 sites high profile enough to appear in Google's email transparency report (as of 2015-09-20):

```
conjur.com.br
mypst.com.br
registro.br
societe.com
t-2.com
bayern.de
bund.de
jpberlin.de
lrz.de
posteo.de
ruhr-uni-bochum.de
tum.de
unitymedia.de
lepartidegauche.fr
t-2.net
xs4all.nl
debian.org
eu.org
freebsd.org
ietf.org
openssl.org
samba.org
torproject.org
isc.org
```

Sites with large # of email users

In terms of volume of email users supported, German sites are far away in the lead, followed by the Netherlands. The rest of the world appears to be testing the waters ..

unitymedia.de
posteo.de
mailbox.org
bayern.de
bund.de
jpberlin.de
lrz.de
ruhr-uni-bochum.de
tum.de
unitybox.de
umbkw.de
nederhost.nl
transip.email

Upcoming: a big announcement for implementation later this year is the from large German EMiG (Email Made in Germany) providers, gmx.de, web.de, 1und1.de, ... that's 10's of millions of users, they're not live yet, but announced in mid August.

Ongoing protocol work

Ongoing Protocol Work

- Message/Object encryption & signing:
  - OPENPGPKEY
  - SMIMEA
  - (These are both close to being published as *experimental* RFCs)

- Newest work:
  - DANE for SIP (Session Initiation Protocol)
  - Client Certificates in DANE TLSA records
  - DANE and DNSSEC Chain Extension for TLS
  - Payment Association Records (PMTA)

OPENPGPKEY and SMIMEA

OPENPGPKEY Record

- Used to publish OpenPGP public keys in the DNS
- Spec not final yet, but RR code (61) already assigned
- Intended status: “Experimental” RFC
  - https://tools.ietf.org/html/draft-ietf-dane-openpgpkey

- Has seen some deployment in the field:
  - Fedora Project: 4,500 keys in the zone (from Paul Wouters).
  - A few other organizations that have deployed or have plans in the pipeline.

Example OPENPGPKEY record

Owner name format:
sha256(username)[0:28]._openpgpkey.<domain>

e.g. for shuque@huque.com

1st label: sha256("shuque") truncated to 28 octets =
adcd5698c7fc6c44e65e893ab7e84a638db4910d04e8e53314e8a101

2nd label: "_openpgpkey"

Remaining labels: domain name portion of the email addr

RDATA is the openpgp key (presentation format: base64)

adcd5698c7fc6c44e65e893ab7e84a638db4910d04e8e53314e8a101._openpgpkey.huque.com. IN OPENPGPKEY <base64 encoding of the openpgp key>

SMIMEA Record

- Using DNSSEC to associate certificates with domain names for S/MIME:
  - https://tools.ietf.org/html/draft-ietf-dane-smime
- S/MIME is a method of encrypted and signing MIME data commonly used in email messages.
- The SMIMEA DNS record proposes to associate S/MIME certificates with DNS domain names.
- Early allocation of an RR type code from IANA has been requested.

SMIMEA record

Owner name format is identical to OPENPGPKEY, except that the 2nd label is "_smimea".

sha256(username)[0:28]._smimea.<domain>

The RDATA format is identical to that of the TLSA record.

(Contentious?) Open Issues

- Email address local-part canonicalization:
  - Punt?
  - Use small set of simple rules?
  - Publish mailbox equivalence rules in DNS too?
  - Don’t do this in the DNS? Use SMTP oracle.

- Privacy leaks of email addresses.
  - Eventual solution to this problem will likely be DNS over TLS:
    - https://tools.ietf.org/html/draft-ietf-dprive-dns-over-tls

Competing idea

- SMTP /Submission Service Extensions for Address Query
  - https://tools.ietf.org/html/draft-moore-email-addrquery-01
  - Query an SMTP server for information about an address (e.g. PGP keys, S/MIME certificates, etc).
  - Preserves SMTP protocol requirement that it alone interprets the local-part of a user address.
  - Uses SMTP over TLS, so can address privacy leakage.
  - Supports clients proxying (AQPX command) request through a submission service (to address possible blocking of port 25).
  - Role of DANE if any (object security assertions?)
  - Non-email application protocols now required to speak SMTP?
  - Unclear how much support there is behind this.

DANE for SIP

DANE for Session Initiation Protocol (SIP)

- A draft proposed in IETF's SIPCORE wg:
  - https://tools.ietf.org/html/draft-johansson-sipcore-dane-sip-00
  - https://www.ietf.org/proceedings/89/slides/slides-89-sipcore-1.pdf

- Use DANE to authenticate SIP target server's cert:
  - Current SIP spec says to authenticate the name in the SIP URI domain (see RFC 5922: SIP Domain Certificates) in URI or dNSName certificate identifiers.
  - This spec proposes to use DNSSEC to follow NAPTR/SRV records and authenticate the TLS certificate at the target server's name via DANE.

DANE for Session Initiation Protocol (SIP)

```
example.com. NAPTR 10 10 "S" "SIP+D2U" "" _sip._udp.example.com.
example.com. NAPTR 20 10 "S" "SIP+D2T" "" _sip._tcp.example.com.

_sip._udp.example.com. SRV 10 100 5060 sip1.example.com.
_sip._udp.example.com. SRV 20 100 5060 sip2.example.com.
```

The SIP DANE draft allows SIP entities to authenticate the server certificate at the target of the the NAPTR and SRV records (in this case the named entities “sip1.example.com.” and “sip2.example.com”, rather than “example.com.”. It is safe to do so, as long as DNSSEC is used to authenticate the NAPTR and SRV mappings.

Client Certificates in DANE TLSA Records

Client Certificates in DANE TLSA Records

- Internet Draft and IETF93 slides:
  - https://tools.ietf.org/html/draft-huque-dane-client-cert-01
  - https://www.ietf.org/proceedings/93/slides/slides-93-dane-0.pdf

- Proposes to:
  - Augment the DANE TLSA spec (RFC6698) to allow TLS Client Certificates to be used in DANE authentication.
  - Specifies additional protocol behavior for TLS clients and servers to use this mechanism.

Authentication Model

- Client has an identity assigned corresponding to a DNS domain name.
  - Not necessarily related to its network layer address(es)
- Client has a private/public key pair and a certificate binding the domain name to the public key.
- Domain Name + Certificate has a corresponding signed TLSA record.

TLSA Record Owner Name Format

```
_service.<domain-name>  IN  TLSA  <..data field..>
```

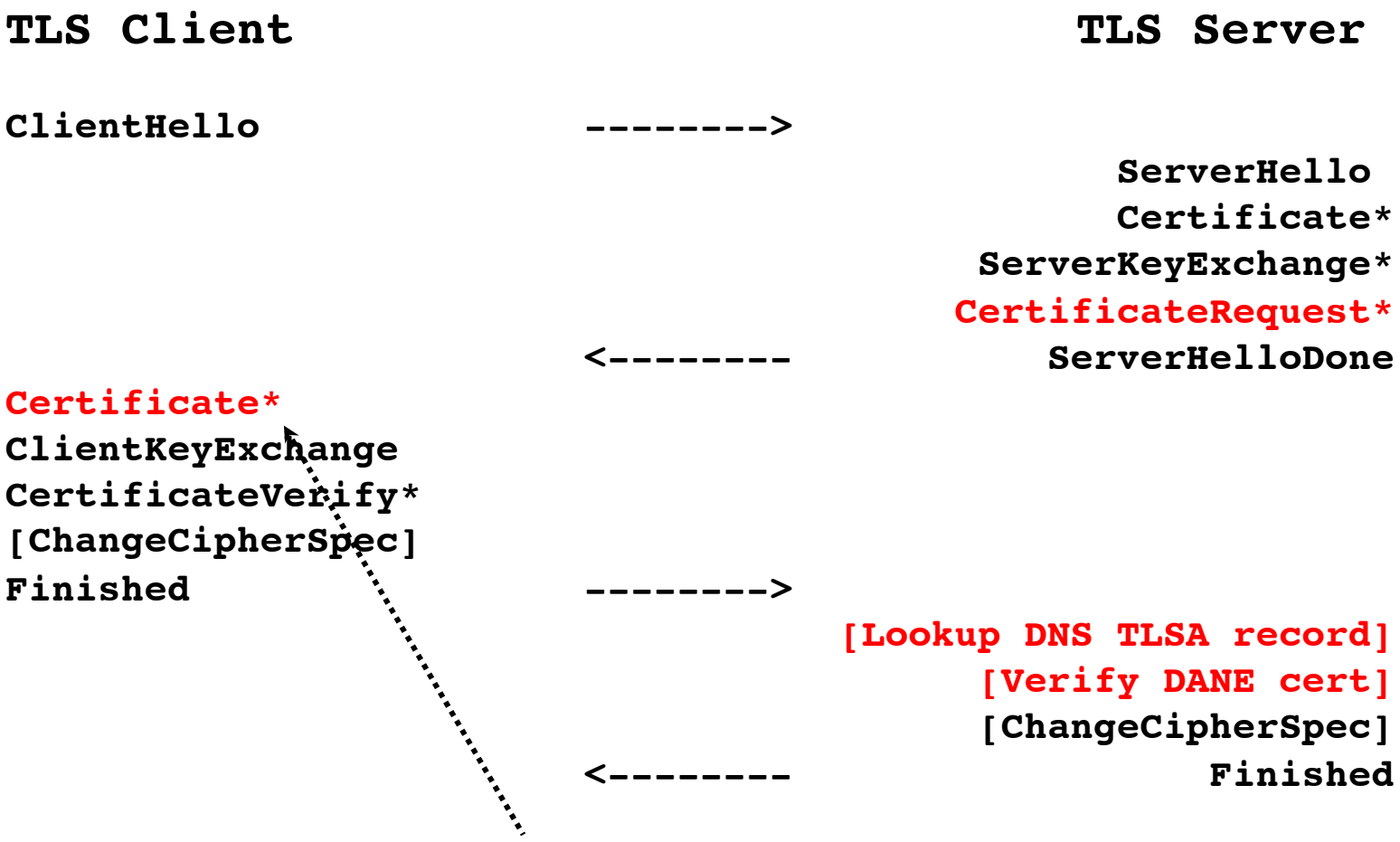
An example:

```
_smtp-client.device1.example.com. IN TLSA (
      3 1 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )
```

Client Identity in Certificate

- Two options in Subject Alternative Name's:
  - dNSName type
  - SRVName type

TLS handshake changes

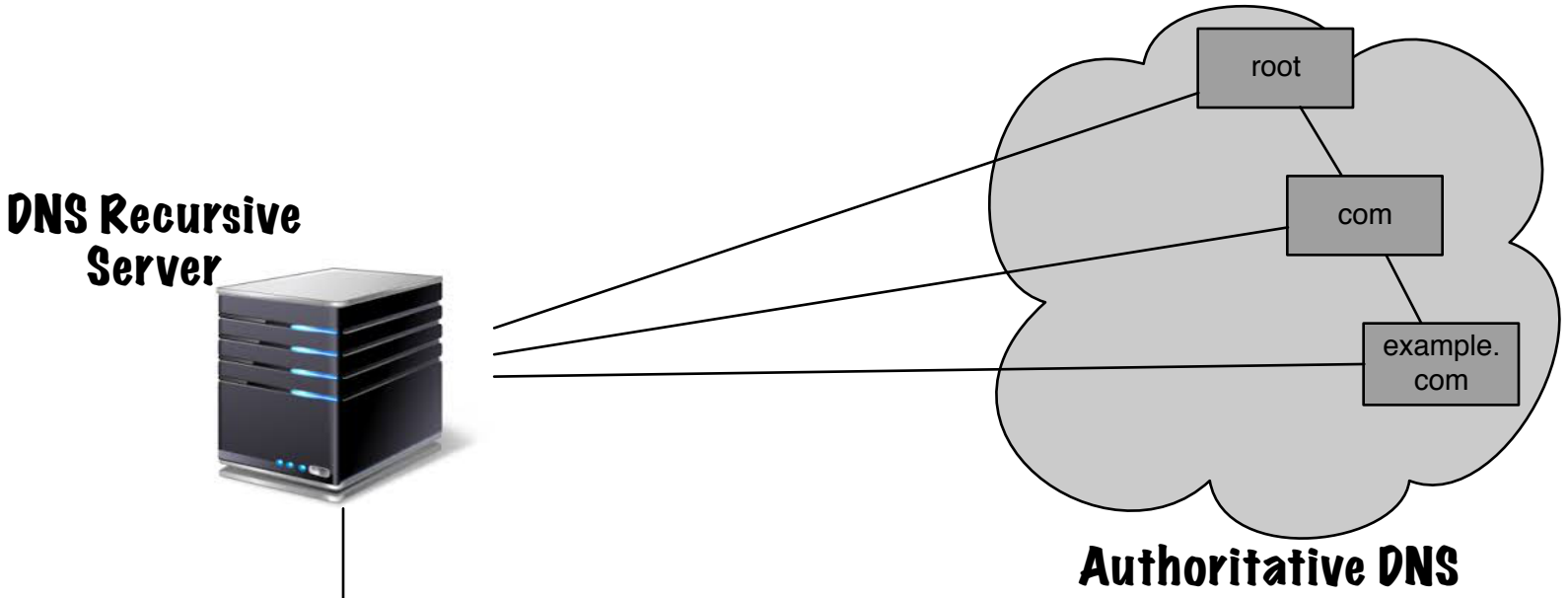


DANE/DNSSEC Chain Extension for TLS

DANE and DNSSEC Authentication Chain

- Internet Draft and IETF93 slides:
  - https://tools.ietf.org/html/draft-shore-tls-dnssec-chain-extension-01
  - https://www.ietf.org/proceedings/93/slides/slides-93-dane-1.pdf

- Proposes:
  - A new TLS extension that allows the server to deliver its DANE record(s) and the chain of DNSKEY and DS records needed to authenticate it.
  - Client authenticates the chain with a locally configured trust anchor, then performs DANE authentication of the server cert.



1

* query DNS
* build DNSSEC chain to DANE record
* Cache and periodically rebuild

TLS Server

TLS Client

3 * Send TLS dnssec_chain

2 * Request TLS dnssec_chain
* Verify chain
* Perform DANE authN

What problem(s) does this solve?

- TLS client doesn’t need to perform the DANE related DNS queries itself.
- Avoids associated latency penalty for those lookups.
- Works around middleboxes that might interfere with attempted DANE/DNSSEC queries.
- TLS client can authenticate the DANE record set itself without needing access to a validating resolver to which it has a secure connection.

Client DNSSEC and DANE Impediments

- Studies have shown that a non-trivial number of clients are unable to successfully perform DNSSEC validation, or even queries for non standard types, because they are behind broken or uncooperative middleboxes.
  - Google's measurements: 4-5% failure rate for queries for non-standard RR types.
  - Willem Toorop's & Xavier Torrent Gorjon, July 2015:
    - "Discovery Method for a DNSSEC Validating Resolver"
    - https://nlnetlabs.nl/downloads/publications/os3-2015-rp2-xavier-torrent-gorjon.pdf
    - RIPE Atlas probe based measurement:
      - 64.71% able to deliver verifiable positive result
      - 55.67% able to deliver verifiable negative result
      - 29.51% able to deliver verifiable wildcard result

Format (in upcoming revision of draft):

```
struct {
        opaque blob <0..2^16-1>;
} ChainData;
```

Opaque blob will be comprised of:

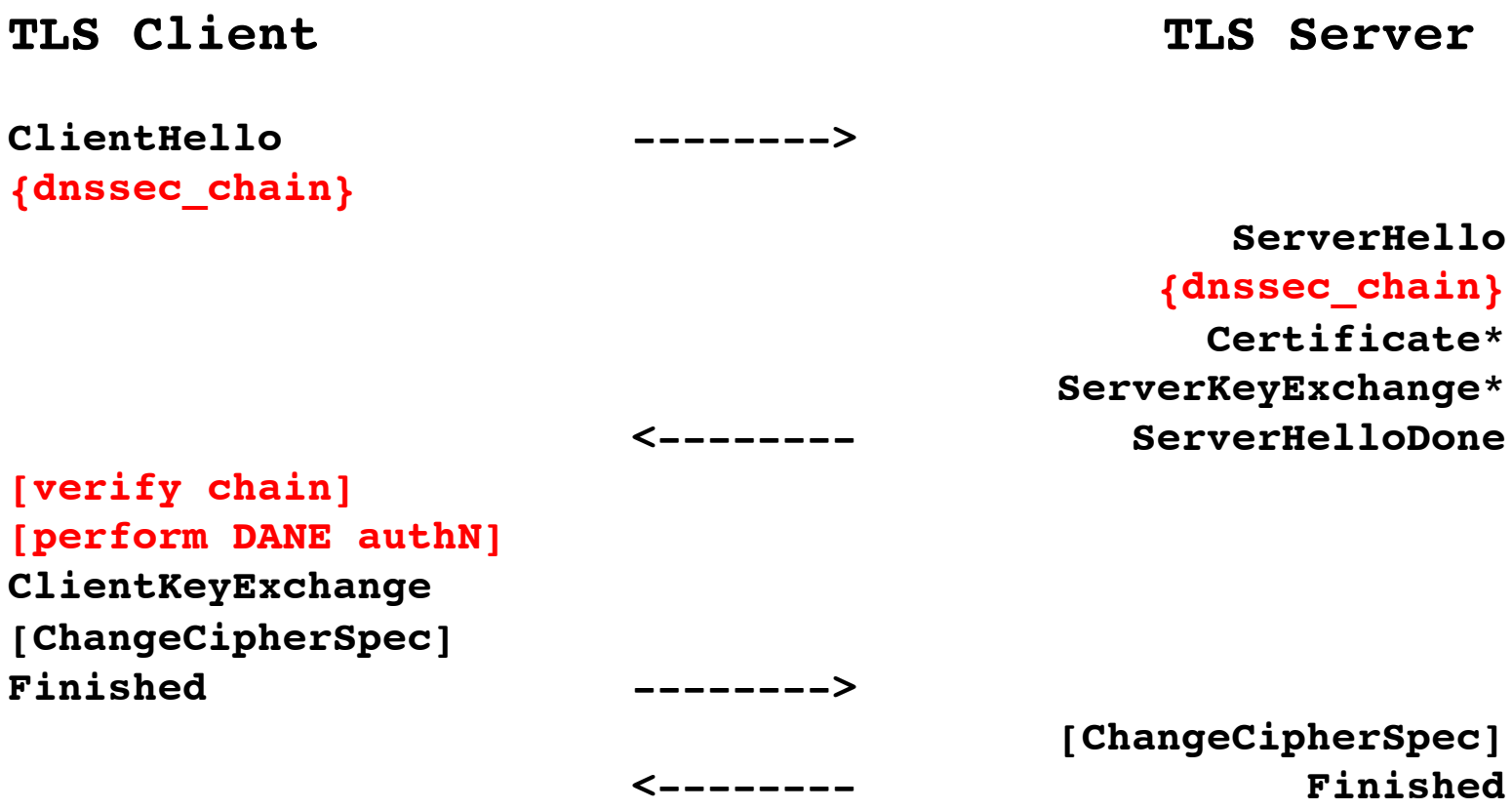
- a sequence of wire format DNS resource record sets
- ordered from the target DANE record to the trust anchor
- signature records follow data records.

An example chain …

For the HTTPS site, www.example.com, with zone cuts at “com” & “example.com”, the DANE chain will include the following order of RRsets (and corresponding RRSIG records):

```
_443._tcp.www.example.com. TLSA
example.com. DNSKEY
example.com. DS
com. DNSKEY
com. DS
. DNSKEY
```

TLS Handshake Changes



Open Issues & Points of Discussion

- Dealing properly with CNAME, DNAME
- Dealing properly with wildcards.
- Best way to do trust anchor maintenance.
- Optimizing the size of the chain.
- Support “Must Staple DANE” assertion:
  - Use new X.509 “TLS Feature Extension”

Payment Association (PMTA)

DANE Records for Payment Association

- Using DANE to associate payment information with email addresses:
  - https://tools.ietf.org/html/draft-wiley-paymentassoc-00
  - https://www.ietf.org/proceedings/92/slides/slides-92-dane-1.pdf
  - Associates an Internet Service identifier like an email address with payment information like an account number or Bitcoin address.
  - New “PMTA” resource record.

- Preliminary implementation work with Armory and Netki
  - DNS provisioning and Bitcoin wallet integration.

What else for adoption?

What else can we do to spur DANE/DNSSEC?

- What other applications need DANE support?
- Better software support for DANE:
  - DANE support in popular SSL/TLS libraries.
  - Use of validating stub resolvers to deliver authenticated DANE records to applications.
  - High performance DNS libraries (async, multiprocessing, pipelining, out of order processing, TFO, etc.)
  - DANE tools.
- General DNSSEC adoption issues?
  - Signing zones & deployment of validating resolvers
  - Middlebox interference issues
  - Key strength issues

Questions or comments?

Shumon Huque <shuque @ verisign.com>

@shuque