

DNS Training – iWeek 2015



By
Mark Elkins
September 2015



DNS
DOMAIN NAME SERVICES

The Intro Course



Introduction

- * Background, why was DNS created (hosts.txt)

Internet before DNS

- * DNS Design Requirements (Extensible)
- * Introduction to the Concept of a "Resource Record"
 - * COZA Limitations
- * Structure Records and Data Records
- * The A and AAAA Records for IPv4 and IPv6 addresses

Caching, TTL and Scalability

- * Delegation, the Key to Scalability
- * The SOA Record: the Start of a New Zone, the Serial Number
- * The NS Record
- * Zones and Domains

Name Server Roles

- * Authoritative Name Servers
- * Iterative Mode Resolvers (aka Recursive Name Servers)
- * Security Aspects and Threats
- * "Cache Poisoning"



Best Practices



- Separate Authoritative & Recursive Servers
- Consider Genetically diverse systems – e.g. BIND & NSD
- Open TCP Port 53
 - Longer replies may be truncated over UDP
- Add rate-limiting to Authoritative servers.
- Read and implement BCP38

Nameserver roles



An Authoritative Nameserver “knows everything” about a zone and can be asked by anyone for information about its zone.

In DNSSEC terms, this is where we "Sign a Zone"

A Recursive Nameserver knows nothing but can hunt down the answer. It should only do this job for a select group of people.

In DNSSEC terms, Recursive Servers do DNSSEC Validation. They Validate what they find.

These two roles **do not overlap**.
They should be **run on separate machines**.



DNSSEC - Validation



The "Trust Anchor" is needed.

```
dig . dnskey | grep -w 257 > root.key
```

Manipulate into the "named.conf" file as:-

```
managed-keys {
. initial-key 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzah0R+9W29euxhJhVVL0yQbSEW008gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIo08g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkj f5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5h0A2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcG0Yl70yQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub80NGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=";
};
```

Stick it just after the "options" section.

For more info - please look at:






<http://dnssec.co.za>

or <http://dnssec.na>



If you use Chrome or Firefox, install the "DNSSEC Validator" Add-on.

Search for "DNSSEC Validator"

-  - Signed and Validates, Chain of Trust is intact.
-  - Signed, but Chain of Trust is broken.
-  - Signed, but does not Validate, Chain of Trust is intact.
-  - Authenticity of TLS/SSL certificate verified by DANE
-  - Invalid, TLS/SSL Certificate does not match TLSA



Root Name Servers

- * The hints file
- * The System Query
- * Scalability
- * Problems with Erroneous Queries, the AS112 Project

Resolvers

- * Stub Resolver and Iterative Mode Resolver
- * Interpretation of Response Messages
- * Recursive and Non-recursive Queries
- * The NXDOMAIN Response
- * Referrals
- * CNAMEs
- * Authority at Delegation Points

Name server implementations

- * New server software and/or new client software
- * BIND (both authoritative and recursive server)
- * NSD (authoritative-only server)
- * Unbound (recursive-only server)
- * Other implementations
- * Differences, pros and cons



IDN, Internationalized Domain Names

- * Problem statement
- * Character codes, Unicode
- * IDNA, Punycode
- * Requirements from and on applications
- * Application support

IPv6 and DNS

- * New data, new record types
- * Nibbles for IPv6 reverse zones, ip6.arpa
- * IPv6 data vs. IPv6 transport
- * The root name servers and IPv6
- * Resolver support

”Reverse delegations”

- * Mappings from addresses to names
- * in-addr.arpa
- * ip6.arpa



TSIG: signing DNS transactions

- * Symmetric encryption
- * Symmetric algorithms: HMAC-SHA1, HMAC-SHA256
- * Securing zone transfers (server-server)
- * BIND: TSIG Configuration in named.conf:
 - * key, server and masters directives
- * Securing the transport vs securing the data

EDNS(0):

- * framework for DNS protocol extensions
- * usage of the OPT pseudo-RR
- * fields in the DNS packet that are expanded via EDNS(0)

Introduction to DNSSEC

- * Background, threat scenario, the Kaminsky attack, etc
- * Walkthrough of the concepts

DNSSEC: Validation of signed DNS data

- * “Trusted keys” and validation of data
- * What does “security apex” mean?
- * And when data doesn’t validate?



DNSSEC: Publication of signed DNS data

- * Asymmetric encryption with public keys
- * Asymmetric algorithms: RSA, DSA
- * KSK and ZSK: different operational uses for keys

DNSSEC: Protocol extensions and new record types:

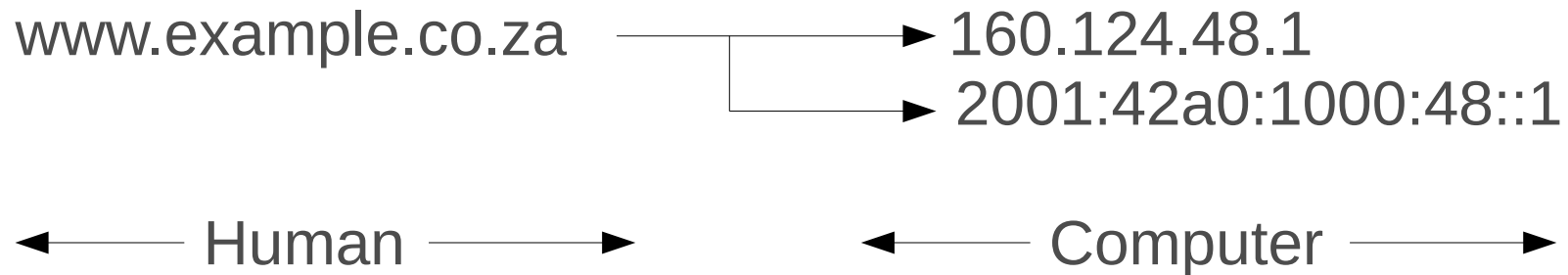
- * RRSIG: digital signature of DNS records
- * DNSKEY: public keys stored and distributed via DNS
- * DS: identification of the "KSK" in use

DNSSEC low-level tools:

- * dnssec-keygen to create keys
- * dnssec-signzone to sign zones



What is DNS?



What is DNSSEC?

DNS – The Reality



DNS relationships are not always so simple.

secdns1.posix.co.za → 160.124.112.10
→ 160.124.208.81
→ 2001:42a0:1:112::10
→ 2001:42a0:1:208::81

160.124.48.8 → café.dnssec.co.za
→ cafe.dnssec.co.za

.



DNS is:

Not designed to be secure
It can be easily spoofed
(the *Kaminsky Attack*)

DNS – Old Injection



Old injection attacks:

www.microsoft.com → porn.com

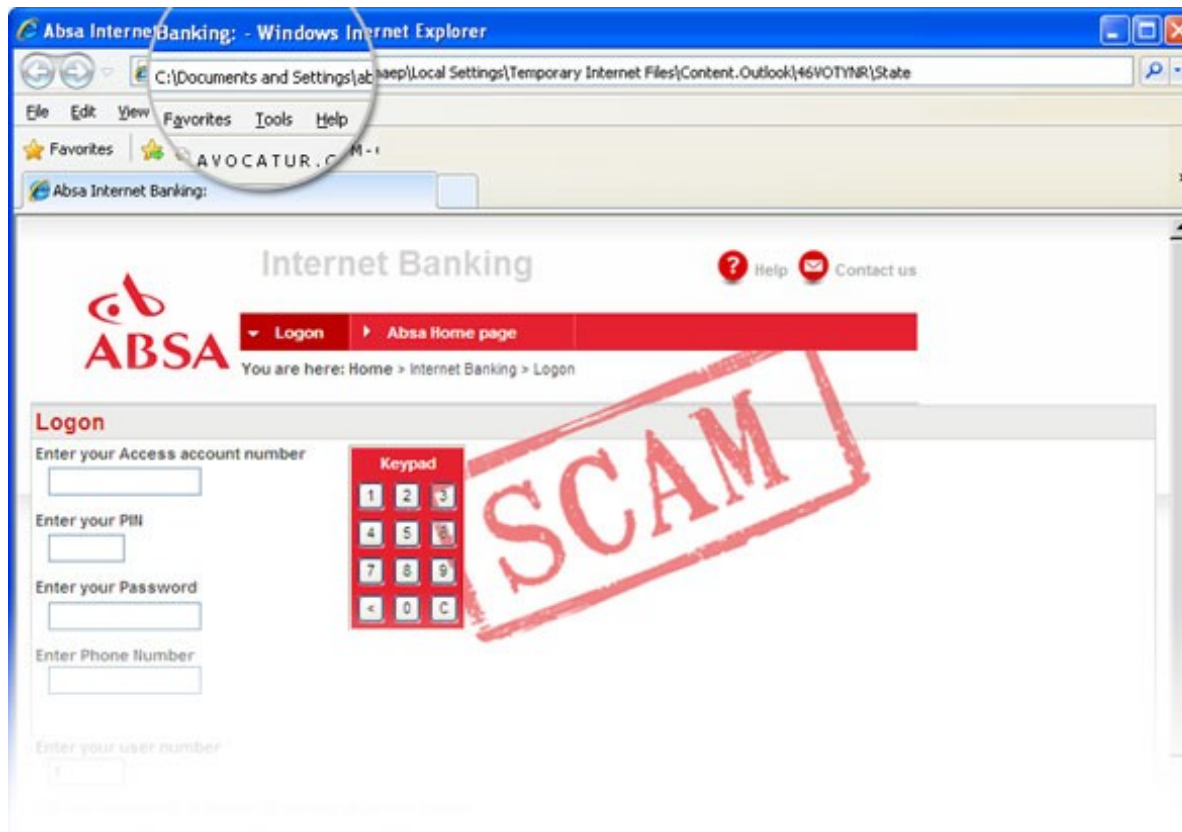


DNS – New Injection



New injection attacks:

www.bank.com → www.fakebank.com





We need a secure DNS
for a secure Internet.



Enter DNSSEC

Available since 2005

Root signed on 3rd March 2010

- i) Zones are Signed
- ii) Lookups follow Signatures

DNS – Unsigned Zone



Zone before signing

Domain “bank.co.za”

www.bank.co.za → 68.177.48.220

mail.bank.co.za → 68.177.48.222

(rest of zone file)

DNSSEC – Signed Zone



Zone after signing

Domain “bank.co.za”

DNSKEY for zone → “The Key”
RRSIG for DNSKEY → “The Signature”
www.bank.co.za → 68.177.48.220
RRSIG for www → “The Signature”
mail.bank.co.za → 68.177.48.221
RRSIG for mail → “The Signature”
(rest of zone file)

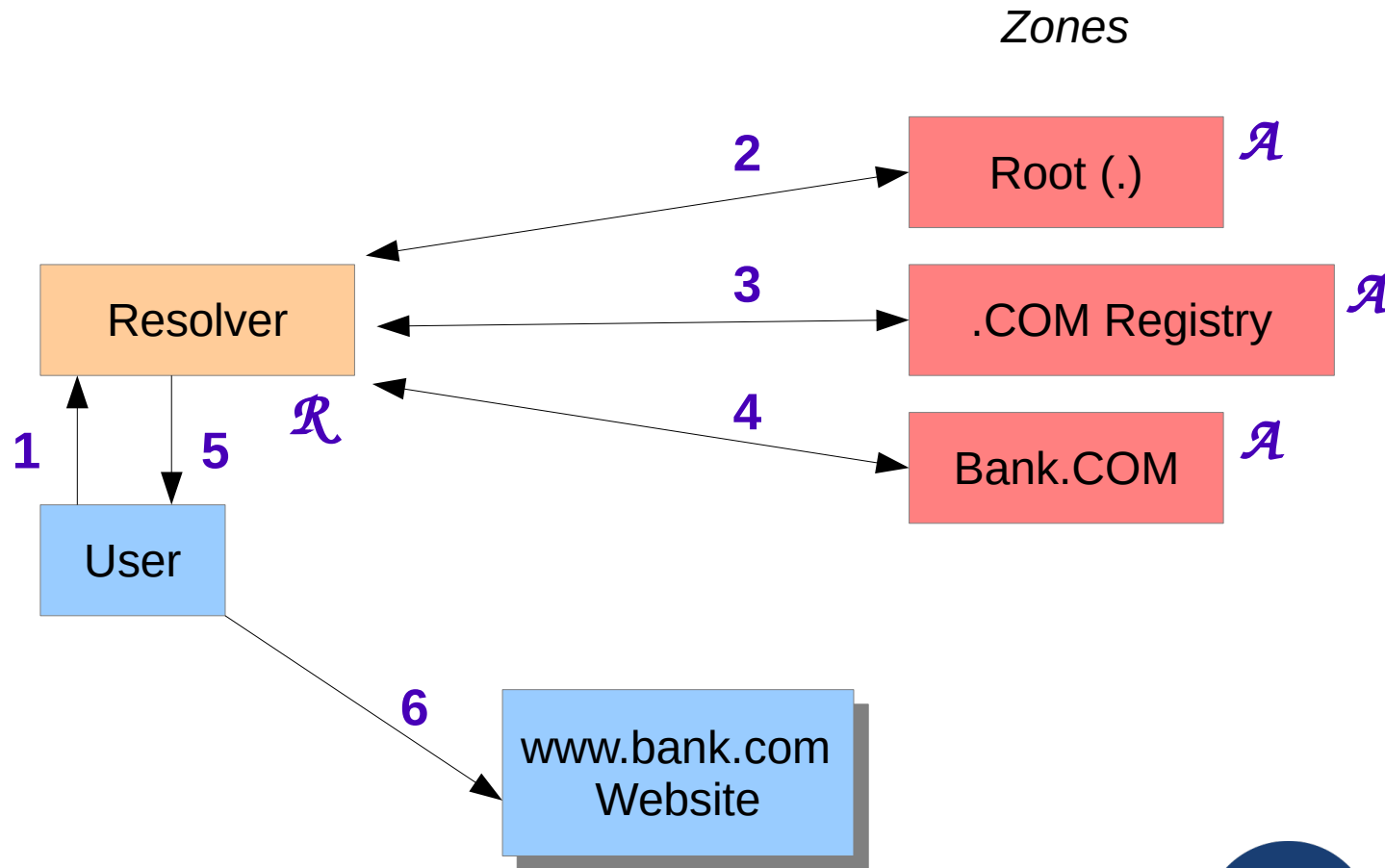
Fingerprint of Key
sent to parent

Signed

DNS – With blind trust



DNS Recursive Resolver

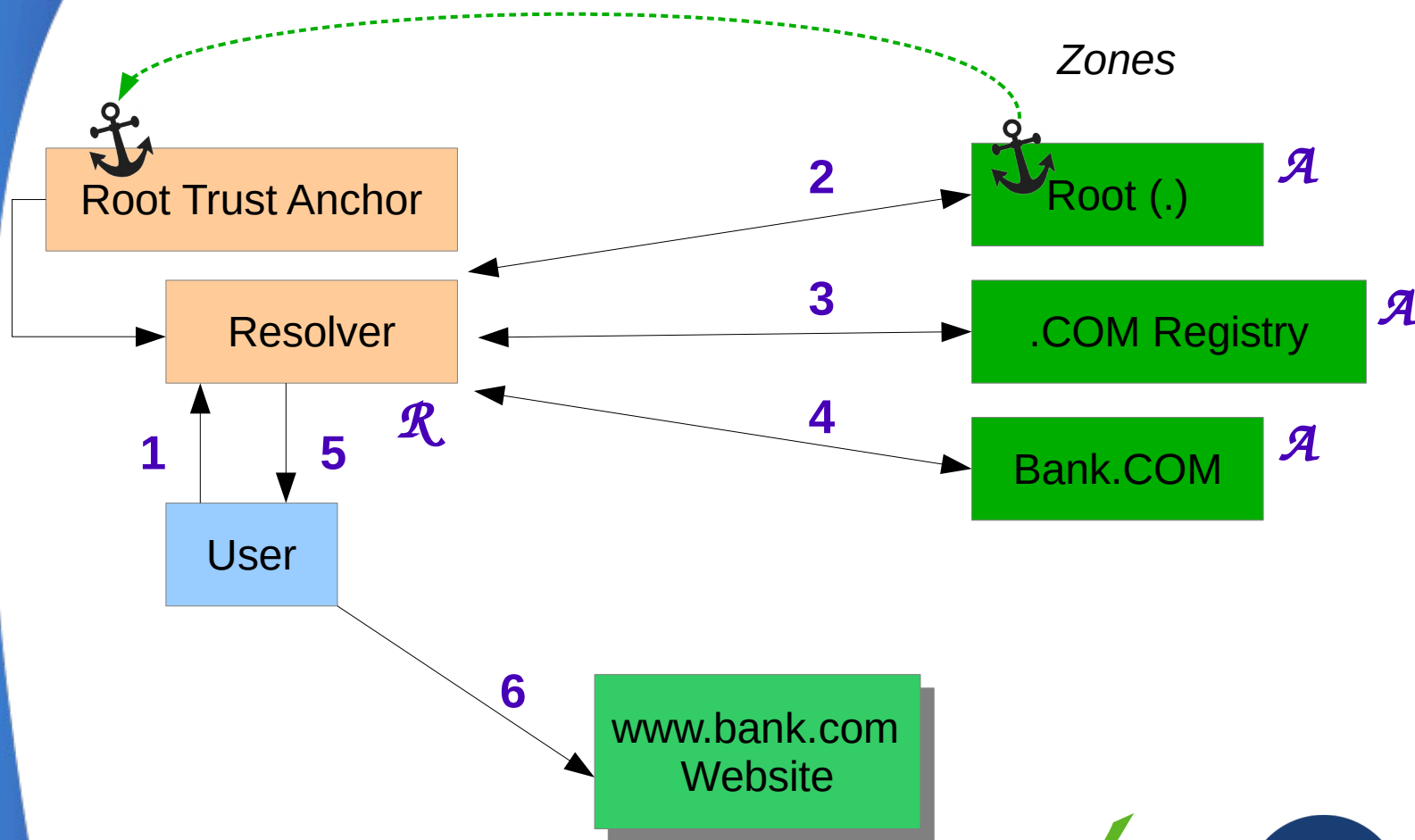


1 – Query: `www.bank.com`
5 – Reply: `www.bank.com 86400 68.177.48.220`

DNSSEC – With verified replies



DNSSEC Recursive Resolver



1 – Query: www.bank.com
5 – Reply: www.bank.com 86400 68.177.48.220



DNSSEC

The User *Gets* what the Domain Owner *Publishes*.

So let's sign...

DNSSEC - Zone Signing



Signing can be quite simple

There are Scripts (eg. mine) (<http://posixafrika.com>)
and black box solutions (eg. *OpenDNSSEC*)

This can be done in just “three commands”
(Assuming you have a zone called 'web.za')

```
# dnssec-keygen -a RSASHA256 -b 1024 web.za
```

```
# dnssec-keygen -a RSASHA256 -b 2048 -f KSK web.za
```

```
# dnssec-signzone -S web.za
```


ZSK - Zone Signing Keys



Its a security key - use secure algorithms

Create it to be flexible in use

Its a security key - longer keys are more secure

Used to sign almost all the data in a zone - so should not be long

Because its not long - should be changed reasonable frequently

Can not change too frequently - to allow for key roll-over

Current wisdom: `dnssec-keygen -a RSASHA256 -b 1024 <zone>`

Length: 1024 bits

Life span: One Month

Algorithm: RSASHA256

Usage: Both NSEC and NSEC3



KSK - Key Signing Key



Its a security key - use secure algorithms

Create it to be flexible in use

Its a security key - longer keys are more secure

Used to sign only a little data - long is fine

Because its long - can be changed less frequently

Current wisdom: `dnssec-keygen -a RSASHA256 -b 2048 -f KSK <zone>`

Length: 2048 bits

Life span: One Year

Algorithm: RSASHA256

Usage: Both NSEC and NSEC3

Zone signing NSEC or NSEC3



NSEC allows a zone to be walked - does this matter?

Small zone with well known information

'za' tld (18 records),
most small websites
reverse IPv4 zone

NSEC3 'hides' the zone content

Large zone with "confidential" information

'co.za' second-level-tld (almost a million records)
large company zones
reverse IPv6 zone

NSEC3 Parameters



Opt in/Opt out

Hash count

10 or less

Prefix,

size - 4 bytes

Regular changes - two weeks

DNSSEC - Zone Signing



'web.za' is now signed and the new zone file is called 'web.za.signed'

There is also a file called 'dsset-web.za.' (*discussed next slide*)

Edit your 'named.conf' to use the new 'signed' version of the zone.

In reality - one should at some regular determined frequency, generate new keys and roll out the old keys....

DS insert in Parent, Chain of Trust

The contents of the file 'dsset-web.za.' needs to be securely installed into the parent zone of 'za'.

```
web.za. IN DS 52867 8 1 921AFBC6DF6....
```

```
web.za. IN DS 52867 8 2 9FBC5FBC6B9....
```

- 1 - Encrypted e-mail (*How I talk to Tanzania*)
- 2 - Via a web front-end (*AFRINIC, Root*)
- 3 - Via the Registries EPP system (*COZA/Cities/.NA*)

Making DNSSEC useful



1 - DNS Security - helps you and your customers to get to the right place. The Internet relies on DNS working correctly!

2 - Certification Security - DANE (*DNS-Based Authentication of Named Entities*)

a) Secure your Web Security Certificate

(so it can only come from your supplier)

b) Create and use your own Certificate (Self-Sign).

3 - Potential other uses:

DANE-for-SMTP-and-MUAs

DANE-for-S/MIME

DANE-for-XMPP (*instant messaging*)

Making DNSSEC useful



www.example.co.za AAAA ??? → 2001:42a0:1:208::13

A Trusted Reply!

_443._tcp.www.example.co.za TLSA ??? → 3 0 1
B635D5DECFF4C30F7DC6606EB12D9CC8C5C05E3F8922
1FE7423AA2D5 AC8CAADA

To generate keys by hand:

Either:

```
openssl s_client -connect www.example.co.za:443
```

Or:

```
cat /home/www/example.co.za/ssl/cert.crt
```

Followed by:

```
| openssl x509 -outform DER | openssl sha256  
(301/web)
```

Or:

```
| openssl x509 -noout -pubkey |  
openssl pkey -pubin -outform DER | openssl sha256  
(311/mail)
```



DNSSEC – TLSA record

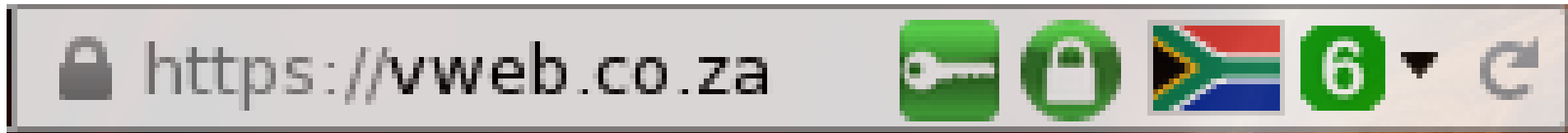


Adding the record

443.tcp IN TLSA 3 0 1 2bc7....7e41

Adding “DNSSEC Validator”

By adding the “DNSSEC Validator” plug-in into the browser we can see full DNSSEC & TLSA Validation



(Yes, I run IPv6)



TLSA

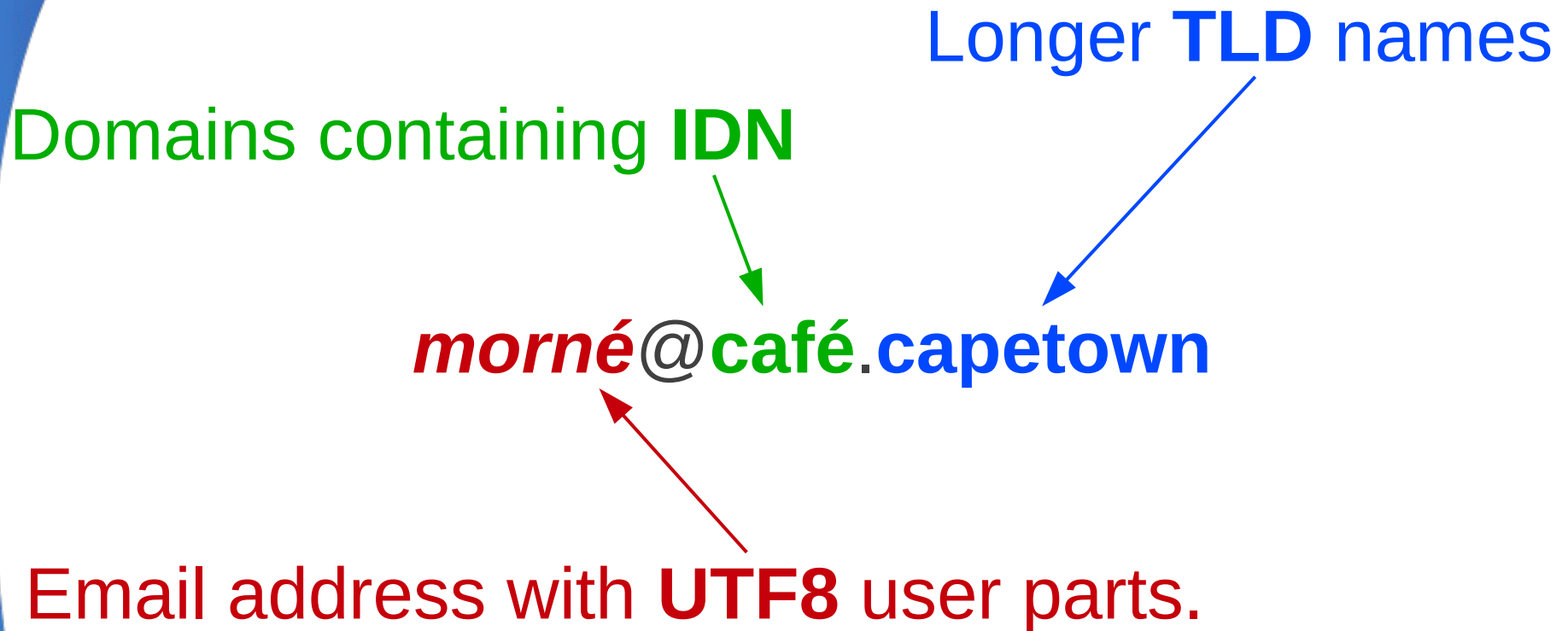
For Web applications:

Users can now verify they have reached the correct Secure Website.

For e-mail applications:

E-mail servers can now verify they have reached the correct destination e-mail server.

DNS – Universal Acceptance





Questions?

Mark Elkins
mark@dns.net.za



DNS
DOMAIN NAME SERVICES