Making the Internet safer for users

Using Let's Encrypt, DNSSEC and DANE

Mark Elkins - mark@dns.net.za

Goals

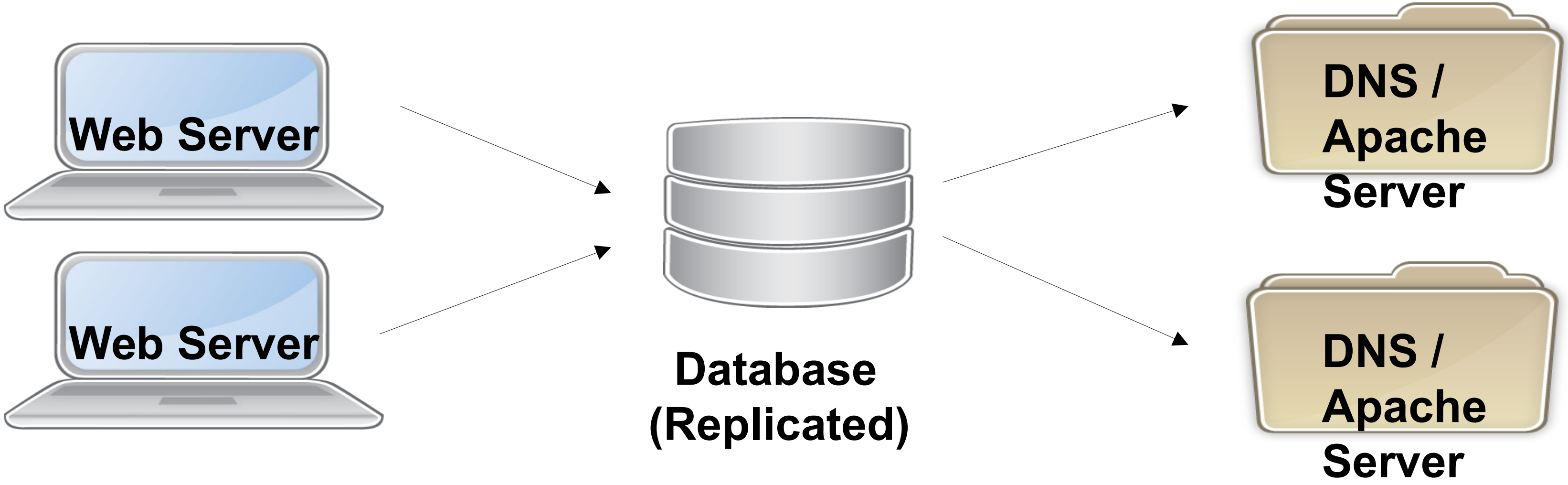
Let’s Encrypt

HTTPS On Everything

DNSSEC on all Domains

DANE TLSA records for Web and SMTP Servers

Environment - for VWEB



- Web and Database interaction is immediate
- A CRON job runs a Synchronisation process every five minutes

Goal - HTTPS On Everything (1)

Let’s Encrypt

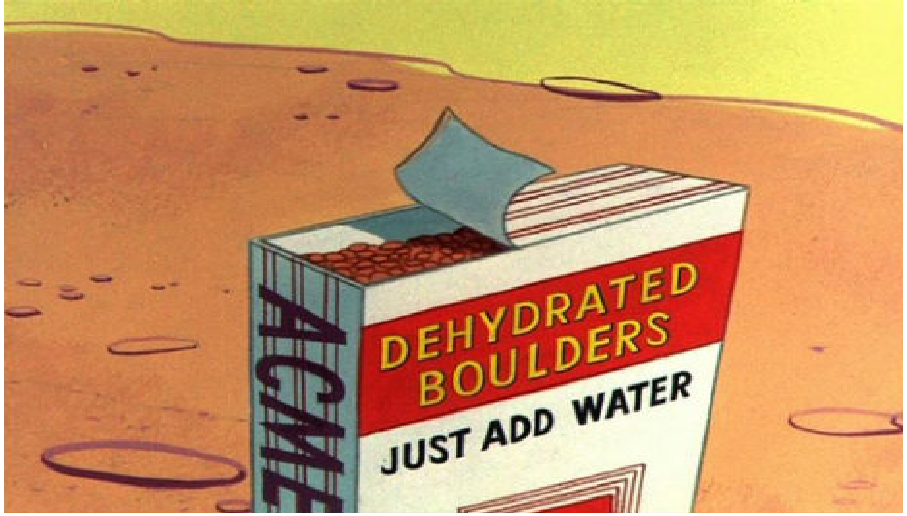
- Free SSL/TLS Certificate service - no costs to hosting customers

- All domains (HTTP -and- HTTPS) can be served from the same IP address (Dual-stacked IPv4 and IPv6)

Could either use HTTP-01 or DNS-01 - chose DNS-01 for verification as:

- More customers run DNS with me
- More in scope with where DNSSEC is intended
- Let's Encrypt will include Wild-cards via DNS validation

Goal - HTTPS On Everything (2)



Use Dehydrated with customised hooks.sh

- Adds TXT token into DNS
- Waits (loops) for it to become visible in global DNS
- Copies completed certificates into VWEB management system

Nightly CRON job to check for any necessary Certificate refreshing

Certificate creation is totally automated, triggered by asking for an Automatic SSL Certificate

- one certificate every five minutes (Dehydrated runs a lock file)
- Limit of about 10,000 domains per server
- Will look at other "Let's Encrypt" implementations

Goal - DNSSEC on all Domain

Securing a Zone means Zone Trust

- Customer always gets the correct Domain to IP address mapping
- Other Information in the zone is also trusted

BASH Shell script using BIND - now five years old - still working

Very liberal KSK roll-over - can take up to six month

- ZACR/DNS runs a well designed DNSSEC implementation using EPP - fast
  - Totally automated Key Roll-over
- AfriNIC/OpenSRS provide a Web Interface for updating
  - Login at a convenient time to do updates
- Others may require an update via e-mail

Changing to include CDS/CDNSKEY support

Looking at Knot DNS - which includes automated Key Management

Goal - DANE TLSA records for Web and SMTP Servers (1)

If you have a Domain Certificate and your DNS is Signed - adding a Fingerprint (Hash) of the Certificate to your DNS should be obvious.

If added for the website:

_443._tcp TLSA 3 0 1 a83b6f1d911e0daf9c...6cff1a51f55d6ae

When the browser looks up the Website IP address, if the website Domain is DNSSEC signed, it should also look for TLSA records. TLSA Records starting with "3 0 1" means the Fingerprint (or HASH) is the hash of the full certificate that should be present, including meta-data such as Certificate expiry date. The browser thus knows what to expect. Depending on user configuration of the browser, the user may not connect to the Website. The user is currently required to install an add-on to obtain this protection - look for "DNSSEC Validator" - https://dnssec-validator.cz

Goal - DANE TLSA records for Web and SMTP Servers (2)

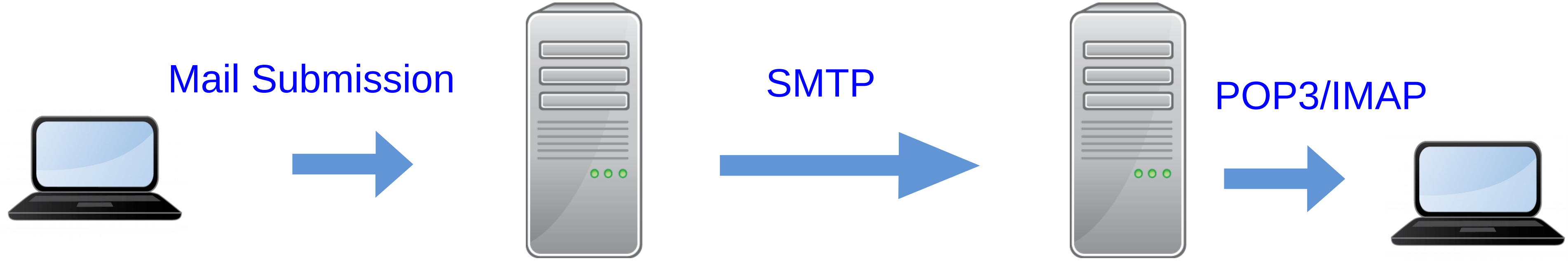
If added for a Mail Server:

_25._tcp TLSA 3 1 1 11abf35f66143af57e...647fbcb26

When a SMTP Mail server looks up the address of another SMTP mail server, if the mail-server zone is DNSSEC signed, it can also look for TLSA records. The TLSA Records starting with a "3 1 1" mean the Fingerprint (or HASH) is the hash of the certificate that should be present, excluding meta-data such as Certificate expiry date. The mail-server thus knows what to expect and will NOT connect if the expected certificate is not there. On a successful connection, the session will be encrypted.

Goal - DANE TLSA records for Web and SMTP Servers (3)

If SMTP Mail servers have certificates, then mail-fetching services such as POP3 and IMAP can work over a secured and encrypted link as can mail-sending services such as Mail-Submission.
Thus, without any User configuration - e-mails can be sent end to end both safely and encrypted.



Questions?

Thoughts?

Let’s Encrypt

DNSSEC

DANE

mark@dns.net.za