

# Certificates and DNSSEC

Jay Daley .nz



# Visiting a secure web site

- Browser connects
- Server sends X.509 certificate
- Browser compares data to web address
- Browser looks for signature of CA
  - If not then this is self-signed
- Browser checks local root certificates
- Browser continues automatically if
  - CA signature matches local root certificate

# Two types of CA signature

- Domain validated
  - This certificate was supplied to the owner of this domain
  - Blue browser bar with domain name
- Organisation validated
  - The owner of this domain is who they say they are
  - Green browser bar with organisation name

# Two related projects

- 1. Using the CERT record for TLS
  - Replacing domain-validated certificates
- 2. TLDs becoming Certificate Authorities
  - Entering the organisation-validation market

# Why?

- ❖ We want our TLDs as secure as possible
  - ❖ Protect reputation of our TLDs
  - ❖ Provide best service to our registrants
- ❖ CA market is failing to deliver
  - ❖ Less than 10% of web sites have protection
- ❖ Certificates are very expensive
  - ❖ Much more than cost of domain name
- ❖ In other protocols security is included

# Certificates in DNS

- Seems obvious to many
- DNSSEC secures the channel
- CERT record already exists
- Change the process
  - Browser does not check CA signature
  - Gets CERT record and compares
- Replaces domain validated certificates
  - Organisation validation still useful product

# CERT might not be enough

- ❖ Lots of CERT records under one domain?
- ❖ What order is it used?
  - ❖ Connect first, get X.509, get CERT, compare
  - ❖ Get CERT, connect, get X.509, compare
- ❖ Too much data? - use a hash instead:
  - ❖ domain            CERT    hash
  - ❖ hash.domain      CERT    ...

# TLD certificate authorities

- ⌚ Entering organisation validation market
- ⌚ Validate registrant identity now
  - ⌚ Are they who they say they are
  - ⌚ CA signature confirms this
- ⌚ Tight process link to domains
  - ⌚ When domain transfer, certificate is revoked
  - ⌚ Also when domain is cancelled
- ⌚ Significant improvement over other CAs

# Ways to enter the market

- ❖ 1. Root certificate in browsers
  - ❖ Expensive verification process (“webtrust”)
  - ❖ CNNIC already there (congratulations!)
- ❖ 2. Buy an intermediate certificate
  - ❖ Not many CAs will sell
- ❖ 3. Shared root certificate amongst TLDs
  - ❖ Each TLD uses an intermediate certificate
  - ❖ Big enough to force browsers to include us

# Next steps

- Two subjects - need two mailing lists
- Certificates in DNS
  - Written to IETF area director
  - Waiting for response
- TLDs as Certificate Authorities
  - Written to ccNSO chair
  - Waiting for response
- Help always welcome!

# Any questions?

[jay@nzrs.net.nz](mailto:jay@nzrs.net.nz)

Or talk to Gihan from .lk

