Certificates and DNSSEC

Jay Daley .nz

p: (+64) (4) 931 6977
e: registry@nzrs.net.nz
f: (+64) (4) 931 6979
w: www.nzrs.net.nz
P.O. BOX 24361, WELLINGTON, NEW ZEALAND
NEW ZEALAND DOMAIN NAME REGISTRY LIMITED

Shameless plug

- ntp.net.nz
- Free NTP service for NZ and Pacific Island network operators
- 3 servers
  - GPS as reference clock
  - Rubidium oscillators for high stability
- High performance
- Managed to internal SLA

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 nae

Problem?

- 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
- Can all CAs really be trusted?
  - Every CA can create any certificate
- In other protocols security is included

Certificates in DNS

- Seemed 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

Current progress

- IETF working group – keyassure
- New protocol and draft – DANE
  - Not PKIX – ignores most fields of X.509
- New DNS resource record – TLSA
  - Different fields to CERT record (simpler)
- Almost done!

Any questions?

jay@nzrs.net.nz

p: (+64) (4) 931 6977 e: registry@nzrs.net.nz
f: (+64) (4) 931 6979 w: www.nzrs.net.nz
P.O. BOX 24361, WELLINGTON, NEW ZEALAND
NEW ZEALAND DOMAIN NAME REGISTRY LIMITED