Certificates, Revocation and the new gTLD's Oh My!

Dan Timpson

sales@digicert.com www.digicert.com +1 (801) 877-2100

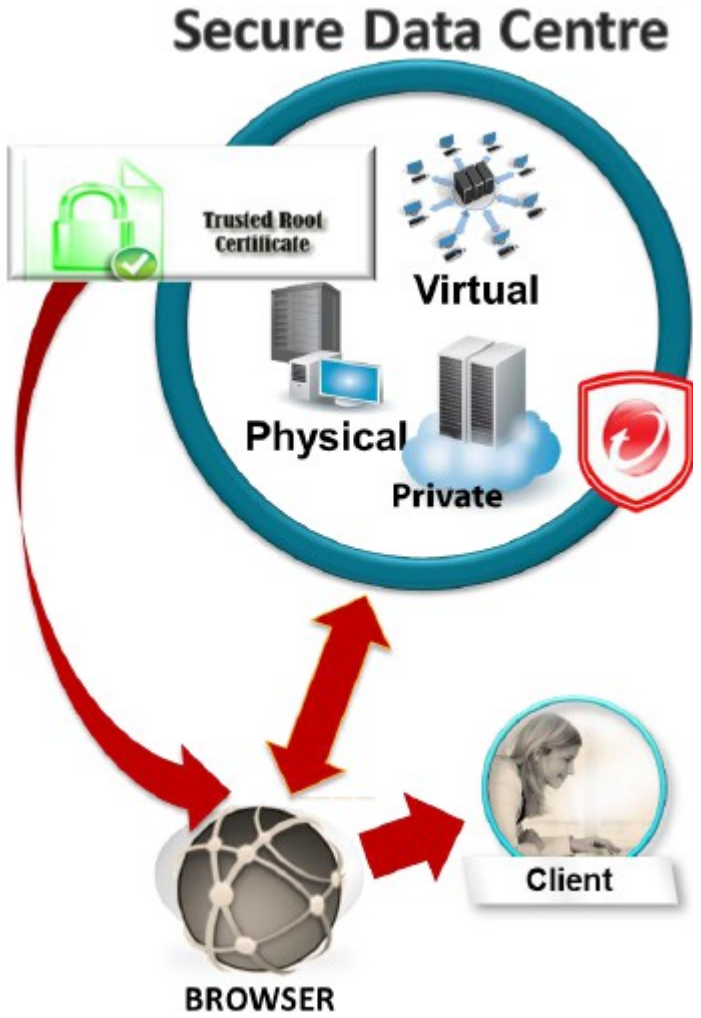
Focus

- What is a Certificate Authority?
- Current situation with gTLD's and internal names
- Action taken so far
- Recommendations

digicert

What is a Certificate Authority?

- CA generates “roots” in secure environment – ceremony, video recorded, audited, keys on HSMs
- CA undergoes rigorous third party audit of operations and policy
- CA private keys are held under extreme protections and used to sign web site certificates and status information
- CA applies for corresponding root certificates to be included into trusted root stores
- CA policy and operations must comply with Browser root store rules in order to be trusted by default - distributed by software updates



What is a Certificate Authority?

- When issuing a SSL/TLS cert to a web site, the CA verifies certain information relating to ownership of the site with the respective domain and verifies control of keys being used.
  - This minimal validation is called **Domain Validation** or DV
  - While DV certificates verify the consent of a domain owner, they make no attempt to verify who the domain owner really is.

- Stronger verification of site and domain ownership and controls for the organizations to which certs are issued allows issuance of higher assurance SSL certificates
  - This additional validation is called **Organization Validation** or OV
  - Additional checks include that they are registered and in good standing with their respective governments etc.

What is a Certificate Authority?

- The strongest verification of site and domain ownership with multiple verification of direct contacts etc., allows issuance of the highest standard of assurance for SSL certificates
  - This highest tier of verification is called **Extended Validation** or EV
  - EV issued certs are recognized in browser GUI e.g. green bar

What is a Certificate Authority

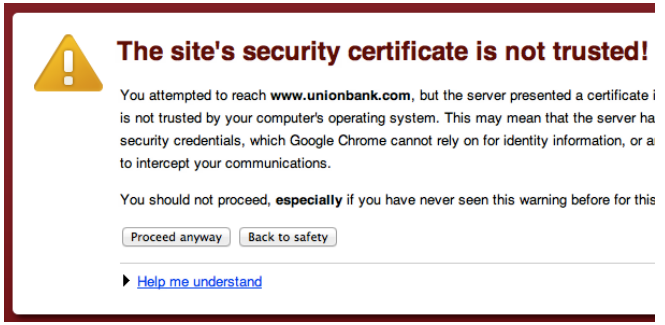
- CA provides certs (**DV** or **OV** or **EV**) to customers chaining to trusted roots embedded in Operating Systems and Browsers
- CA Customers (Site Operators) install certs on their servers for secure web pages
- Users (clients of CA Customers) go to secure web pages **HTTPS://**, User Agent checks for CA's root inclusion in browser trusted root store
- If CA's root is in browser's trusted store:

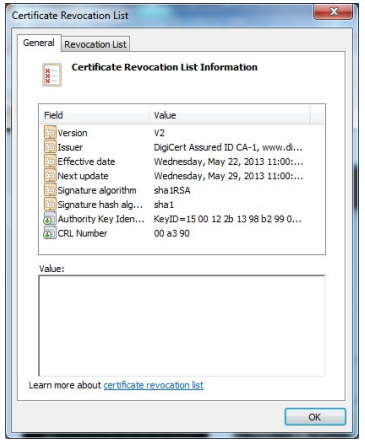
  encrypted session, favorable padlock

  UI (including EV green bar)

What is a Certificate Authority

- If CA root not in client trusted root store for browser – warning displayed
- CAs and browsers have the ability to revoke roots, sub-CAs, and certificates for any problems
- CAs publish revocation lists (CRLs) or provide updated certificate status information online (OCSP)
- If certificate revoked or expired – warning displayed
- CAs must complete annual audits and follow CA/B Forum rules to remain in browser trusted root stores
- Stronger rules and higher CA standards are set for green Extended Validations or “EV” display





digicert

Revocation info

- All browsers perform some level of certificate revocation checking
- All CA's must provide revocation information via OCSP
- OCSP cache times vary by browser with the longest cache time of 7 days
- OCSP stapling provides OCSP response with the certificate
  - Most current server distributions support stapling

Background - Internal names

- Prevalent use of internal name certs
- Estimate is ~11,000 certificates issued against internal names
- Common/recommended practice until 2011

Why is this a problem?

- Collisions
  - Many servers are configured this way
  - Different experience externally
- Security
  - Potential for man-in-the-middle attacks
  - 5 year attack opportunity on organizations with that domain

Action taken so far

- CA/B Forum's original baseline requirements mandated that all internal certs expire or are revoked by 2015
  - Based on server operator feedback and businesses
    - Roadblocks include policy, cost and training
- CA/B Forum approached by ICANN
  - CA/B Forum passed a ballot – Feb 20, 2013
  - Accelerates the deprecation from 5 years down to 120 days after the relevant gTLD contract is published.
  - 120 days is required for large volumes (Top 10%)
- Mozilla.org has adopted the revised requirements
  - July 31st All CA's must comply to remain in the trust store

Action taken so far

- CASC – Was formed by CA's to improve education, marketing and research
  - Information on OCSP stapling
  - Reconfiguring servers with public FQDN's
- Avoiding Collisions
  - Digicert and other CA's are actively working to migrate customers off internal names
    - Communicating with customers
    - Only solves training doesn't reduce cost
    - Digicert Internal Name Tool

Recommendations for ICANN

- Don't approve the names that are most commonly used in internal certs until 2015
  - Digicert Letter (.corp gTLD)
  - PayPal letter
- Approve the application but delay the delegation until 2015
- Remaining 90% can move forward with minimal impact
- Security issues with certs is effectively resolved