Web PKI: Background and Issues
Web PKI Operations BoF (WPKops)

Jeff Hodges
Brad Hill
PayPal

IETF-85 Atlanta
5-Nov-2012
What is the “Web PKI”? 

• The Public Key Infrastructure (PKI) that is
  – Embedded in various software packages/components..
    • HTTPS clients
      – Notably Web Browsers
      – Operating Systems, Mobile Apps
      – OpenSSL, curl, wget, Java, Ruby, Python
    • Web Servers
    • Certification Authorities
      – Deployed pervasively across the Internet
      – Highly user visible
      – Depends upon a particular (complex) object shared amongst participating software: *Public Key Certificates*
The Players

• End users
  – “Are there any issues with my present use of this web app? Is it secured?”

• Certificate Holders
  – AKA “web application providers”

• Hardware & Software Providers
  – E.g. Browser vendors, web server vendors, TLS/SSL Concentrators etc.

• Certificate Issuers
  – AKA certificate authorities (CAs)
Web PKI Issues

- There are issues with the presently-deployed Web PKI affecting all the players:
  - Web PKI is specified in IETF PKIX specs
    - Which profile ITU-T X.509 specs
    - Originally concocted in mid-1990’s (pushing 20yrs)
    - All these specs have evolved
    - Complicated; many “options”
    - Prone to interpretation by implementers in various places
Web PKI Issues [2]

• WebPKI-encompassing software packages/components have:
  – Evolved over time
  – Individual interpretations of PKIX specs
• Yields user-visible inconsistent behavior
Web PKI Issues [3]

- Certificate holders (Web App Providers)
  - Uncertainty regarding user agent behavior relative to:
    - Web App’s presented certificate & cert chain
    - CA’s OCSP/CRL services
  - Can result in:
    - different user experiences between UAs
    - some users not being able to use web app
    - Security vulnerabilities
Web PKI Issues [4]

• Certificate Issuers (CAs) challenges regarding:
  – Certificate complexities
    • accurate/correct AIA info
    • Subject naming conventions
  – CRL and OCSP content/operational complexities
    • Which clients accept what spec interpretations?
    • E.g., necessary to include nonce in OCSP response?
    • Client cert chain processing peculiarities?
Web PKI Issues [5]

• End users
  – Inconsistency across browsers in terms of
    • Behavior given cert contents, cert chain, and cert status checking
    • Security indicators
  – Web apps “breaking” due to impedance mismatch between
    • presented cert(s) + revocation infrastructure
    ..and..
    • browser implementations
Web PKI Issues [6]

• Multi-stakeholder
  – Revocation checking and performance
    • As a cert holder, what is your CA doing?
    • How does that really affect performance for your clients?
    • GET vs. POST, cache-ability of responses
    • Impact of / requirements for Stapling
  – IDNA
    • Different versions
    • Complex chain of rules/validation between registrars, CAs, certification validation code and URL bar display rules
Example Issues to Survey

• Criticality of the nameConstraints extension
• Use of the OCSP "good" certStatus value
• Behavior of IRIs, IDNA 2003 vs. 2008, Unicode restriction profiles