Standards for the Web PKI

Tim Moses

IETF 84, Vancouver Aug 2012

IP

- To the best of my knowledge, nothing mentioned here is encumbered by claims in a patent or patent application

Let a thousand PKI specs bloom

- PKIX
- SPKI
- PGP
- ISO 7816
- Web PKI

Web PKI

- Not just a PKIX PKI gone wrong
- Size and age make it a distinct type of PKI

Characteristics

- First introduced in 1994
- Two billion relying parties
- One million subscribers
- A dozen Policy Management Authorities
- Hundreds of CAs
- Every country in the world

Shortcomings

- These are well-known

Remedies

- Establish minimum security requirements within the existing trust model
- Augment the trust model

Principal specifications

- RFC5280 - Certificate and CRL profile
- RFC5019 - Lightweight OCSP profile
- RFC3647 - CP and CPS framework

Variations

- Result from:
  - Technical limitations in deployed clients
  - Incompatibility with strategic direction of PKIX WG
- Even 1% represents 20 million users
- Examples:-
  - Criticality of the nameConstraints extension
  - Use of the OCSP "good" certStatus value

Need for a citable specification

- Accurate record of how the Web PKI ACTUALLY works
- Discuss and agree future evolution of the Web PKI
- Starting point for developers of new Web PKI clients

Proposal

- Form a working group within the Operations and Management Area

- Catalog the Web PKI's known failure modes

- "Profile" existing IETF specifications (with non-conformant variations essential to the Web PKI)

Next step

- Gauge support for a BoF at IETF 85