Harmonizing PKIX and DANE

Richard Barnes
BBN
DANE @ IETF80
How TLS works today
The question for DANE

DANE

Application

PKIX cert/path validation

TLS Cert Chain

TAs

Policies

Accept/Reject
Goals

• Define how DANE affects TLS certificate chain validation
• Modify PKIX inputs, not PKIX process
• Enable the use cases the WG has agreed on
Definitions

• “CA-issued” certificate:
  A certificate issued by an entity other than the domain owner (e.g., a commercial CA)

• “Domain-issued” certificate:
  A certificate issued by the owner of a TLS server and its domain name
  – Example: self-signed certs and their children
CertType 2 is fine

- With CertType 2 (CA certificate), there is no ambiguity in how to apply PKIX
- The certificate in the DANE record is used as a trust anchor in PKIX
- One subtlety:
  - PKIX TA = name, key, key params
  - No other checks required by PKIX
    - But several are common; signature validity, expiry
    - DANE could require some of these additional checks
What about CertType 1?

• The intended semantic is that the server cert MUST be the same as the DANE cert
  – Is this necessary or necessary+sufficient?

• Spectrum of options here:
  – One end: Full PKIX validation
  – Other end: Bare keys
  – Middle: Bare keys + some PKIX-like checks
    • Omitted for simplicity
Option A: PKIX Validation

• TLS cert MUST match DANE and pass PKIX validation (including chaining to a TA)
• For CA-issued certs, this pins the cert
  – Guards against re-issue by the same CA
• For domain-issued certs, also need a CA to chain to
  – Self-signed certs are CA certs
    • Not legal for TLS
  – Domain-issued CA cert in a CertType=2 DANE record
Option B: Bare Keys

• Current document uses cert that are never validated by a relying party
  – A cert that’s not validated is invalid
  – Unfriendly to PKIX
• Instead, just encode what you care about
  – Public key
  – (Anything else?)
• For CA-issued, useful for DANE with backward compatibility
• For domain-issued, still need to generate and keep a cert for TLS
## Comparing the options

<table>
<thead>
<tr>
<th></th>
<th>A. PKIX</th>
<th>B. Bare Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain-issued</strong></td>
<td>Requires second certificate (CA) in a Type 2 record</td>
<td>Still need to generate and store cert for TLS</td>
</tr>
<tr>
<td><strong>CA-issued</strong></td>
<td>Useful for deploying DANE while preserving backward compatibility</td>
<td>Guards against CA issuing a second certificate to someone else</td>
</tr>
</tbody>
</table>
Summary

DANE

CertType = 2
(CA Cert)

CertType = 1
(EE Cert)

PKIX Validation

Bare Keys
Gedankenexperiment

• Should you accept …
  1. An expired certificate?
  2. A certificate with incorrect CA bits?
  3. A CertType-1 certificate with a different domain name