Public Key Pinning

Chris Palmer and Ryan Sleevi
Google, Inc.

Changes since draft-02

- Clarified support for SubjectPublicKeyInfo where some parameters are implicit from the chain, such as DSA keys (conclusion: not pinnable, ignored in pin evaluation)

Open Issues - Issue 53

Private / Enterprise / Local Policy-defined PKIs

- Is pinning meant as an protection for all PKIs, or is it meant as a defense in depth for the public/"web" PKI
- Enterprise Proxy vs DigiNotar
- Should / can implementations make a distinction between publicly trusted PKI ("Web PKI"?) and private/application-defined PKI.
- Should / can applications make a distinction?
- Normative / Informative behaviour regarding pin validation failures in these cases

Open Issues - Issue 54

- Reporting & Reporting-only mode
  - Modeled after Content Security Policy's report mode
  - Should there be a report mode?
  - What information should be reported?
    - Received certificate chain?
    - Client-constructed/validated certificate chain?
    - Active pins at the time of failure?
  - What may be configured by the host?
    - Should there be a well-known URI, or should it be configured in-band in the header?
  - If report URI is HTTPS, how to handle connection, trust, or policy errors?

Open Issues - Issue 55

- Interaction with Preloaded Pin Lists
  - Intended to be editorial in nature
  - If a pinning directive received via header conflicts with an internal/preloaded pin list, including a directive to disable pinning (maxAge=0), UAs must use and enforce the most recently received directive, rather than the preloaded directive.

Points of Future Consideration

- Interaction / intersection with RFC 6698 / DANE usage types 0 and 1
- If the TLS WG adopts TACK as a WG Item, interaction / intersection with TACK