Certificate Reference Extension

Phill Hallam-Baker
VeriSign

Objective: Link a DKIM key to a certificate

- Allows use of Trusted Third Party Accreditation
  - Key holder X is accountable (EV)
    - Key holder X is company Y incorporated in Z
  - Key holder X has a certified (good) reputation
  - Key holder X has brand identity logo **NIST**

Technical

- Extension to Key Record
  - Choice of tag name [of no consequence]
  - Value MUST be URI locator
  - Choice of content type: Certificate or Certificate Chain
    - Other assertion formats can make separate proposal
- Pointer to certificate
  - X509=http://example.com/2008/dec1.x509
- Pointer to certificate chain
  - X509Chain=http://example.com/2008/dec1.x509cms