Entity to Entity

Phillip Hallam-Baker
VeriSign Inc.

Objectives

- Mitigate phishing attacks
  - Need to give useful instructions to users
  - Bind a brand logo to a signature
- Create signed email market
  - Make it easy and free to sign email
  - Get past the S/MIME vs PGP standards war
  - CA services are a premium service for the few

Problems with S/MIME (Abridged)

- Unacceptable end user experiences
  - Sender cannot predict which 5% have one
- Signatures are optional
  - Lack of signature is never significant
  - No way to say bigbank.com signs everything
- End-to-End or nothing attitude
  - Leads to nothing
  - Domain based security is wildly successful

XKMS 2.0

- Key Centric PKI
  - W3C Candidate Recommendation
  - A Web Service (first ever!)
  - Comprehensively reviewed by PKI world
- Manages the whole key lifecycle
  - XKRSS – Key registration
  - XKISS – Key Information
- A three year effort, practically complete
  - Deployed with real world experience
  - All we need to do is define a URI for our spec

Alternatives to XKMS 2.0

- WS-Trust
  - Not in standards process
  - Only addresses part of XKISS functionality
  - Is designed to meet needs of Web Services
- PKIX SCVP
  - Designed to deliver X.509 certificates
  - Not what people here want
- Something new
  - Will be a three year journey.
  - Most likely to end up with a Web Service….