PKNG

PKI THE NEXT GENERATION
THE SEARCH FOR PKI
THE WRATH OF PKI
PKI VOYAGER

TERENA TF-EMC2 WIENNA 2010
http://www.terena.org/activities/tf-emc2/meetings/15/
Leif Johansson - leifj at sunet.se

Coordinates

- pkng@irtf.org
- http://www.irtf.org/charter?gtype=rg&group=pkng

Ground Rules

- Listing Desired Features, Not Requirements
- Formats and Protocols Come Last, If Ever
- This Effort Is Not About Criticizing PKIX
- We Are Doing Research, Not Engineering

http://trac.tools.ietf.org/group/irtf/trac/wiki/pkng

Some Themes so far..

Bottoms-up vs Top-down

- In a traditional PKI trust is built top-down
- The IM buddy-list and PGP represents a form of trust that is bottoms-up.
- SAML metadata has aspects of both top-down and bottoms-up trust.
- Maybe PKNG is both...

Usability and Deployability

- Using PKNG in applications must be easy.
- There should be a way to transition from PKI to PKNG – Might A PKNG *something* look like an X.509 cert?
- Adding trust (crosses and bridges in the X.509 model) must be easy even after a PKNG *something* has been deployed.

Out of this world

- Delay Tolerant Networking
  - http://www.dtnrg.org/wiki
- Quantum Resistant PK Crypto
  - Google Lamport Signatures and be Afraid, Be Very Afraid!
  - http://middleware.internet2.edu/idtrust/2009/program.html

Unsorted

- Soft failure modes – not just accept/deny for keys
- Handle inacurate clocks
- Split keys (cf root dnssec key ceremonies)
- Selective field visibility for RPs

Whats it to us (The R&E Federations)?

- Supporting multiple technologies (SAML, OpenID, Information Card) implies supporting multiple technical trust frameworks.
- We need build scalable bottoms-up trust before our metadata files grow beyond our ability to manage them as flat files.

?