



Shib and PKI – “a many-splendored thing”

Ken Klingenstein
Director, Internet2 Middleware and Security

- PKI within Shib
 - enterprise to enterprise
- Using PKI credentials with Shib
 - For high LOA
 - For privacy, for attributes
- Using Shib to get PKI credentials
- PKI and Federated trust frameworks and their overlaps
- Some non overlaps – signing, encryption on an individual level



PKI within Shib

- Shib is, in some sense, enterprise-based PKI-signed assertions.
- The hardest part of installing Shib is getting the PKI right...
- Active discussion about containing raw keys in the metadata as an option to certs

Using PKI credentials with Shib

- PKI cert as end-entity act of authentication
- For high LOA
 - The power of the physical possession and on-card crypto capability
- For privacy
 - Keep identity local to the IdP if desired
 - Secrecy as the flip side
- For attributes
 - Dynamic by nature; attribute certs vs SAML
- For peer-peer exchanges of federations
 - Avoid path construction and validation
 - Avoid bridges, we think

Using PKI credentials with Shib

- Some issues
 - Introduction of enterprise as middle-man
 - Introduction of federated operator(s) as tertiary middle-men

Using Shib to get PKI credentials

- The “Shibbed” CA
- Growing popularity in Grid space
 - Intention to issue a IdP set of guidelines to meet IGTF acceptability
 - Several incarnates
- Really a part of the missing “credential convertor”
- SASL-CA and the use of Shib by devices

PKI and Federated Trust

- Conservation of policy authorities for trust
- Sharing overhead of identity-proofing and maintaining enterprises
 - Initial ID
 - Regular audits, etc
- Branding a common service
- Correlating practices and LOA's, etc.
- Peering of federations
 - Policy? Technology?

Clear distinctions, kind of...

- PKI for signing
 - But if in an enterprise-enterprise context, maybe the Ander's rant...
- PKI for encryption
 - But the escrow issues may be enterprise
- PKI for end-end assurance