



Trust Management in Shibboleth and InCommon

RL “Bob” Morgan
University of Washington and Internet2
TERENA TF-EMC2
Florence, Italy
March 2007

- really “identity management” for peer entities
 - names, roles, keys, capabilities
 - range of LoAs possible, just like with people
 - support varies widely in products
- SAML defines “metadata” format
 - generally service description format, examples in other technologies such as WS-SecurityPolicy
 - better than “via out of band agreement”
 - better than peer-description format per product
 - doesn't replace product local configuration

- plugin API for “trust engines”
 - decide on validity of signature on signed object (usually a SAML assertion)
 - decide on validity of cert (usually for TLS)
- trust engines in Shib 1.3
 - “shibboleth trust engine”
 - PKIX-based validation, using platform PKIX services
 - keys/CAs listed in metadata
 - “basic trust engine”
 - key-matching validation, using keys listed in metadata
 - generally in certs, but no processing of cert controls

INTERNET²® Benefits of PKI (for SAML trust mgt)

- standardized validation, path construction
- lifecycle management
 - validity periods, key rollover, revocation
- flexible naming (DNs, altNames)
- extensibility
 - via adding elements to cert
- platform support
- many existing CAs

- naming
 - DNs confusing, altNames not well-supported across platforms, tools
- key-usage bits, etc, can be trip-ups
- path processing inconsistent across platforms
 - eg openssl handling of cert chains
- keystores hard to use for sysadmins
- no general-purpose cert-acquisition infra
- unknown practices at commercial CAs
 - designed to serve SSL web server market

- Many federations run fed-specific CA
e.g., InCommon, US E-Auth
to simplify trust base, vs using general-purpose CA
but: adds PKI complexity, loses benefit of use of existing
CA infrastructure
- peer joining federation often has to get new cert
either from fed-specific CA or commercial CA used by
federation
this is obstacle for some sites

- all key-handling in metadata?
 - metadata can do this (in Shib), with basic trust engine
 - metadata is essential part of trust base even if PKI used
- benefits
 - works consistently across all Shib deployments
 - works consistently across (all?) vendor products
 - no CA ops required
- encryption
 - useful in three-tier, other scenarios
 - probably means keys in metadata to work

- lifecycle?
 - validity can be expressed in metadata
 - rollover / revocation handled
 - requires metadata refresh by participants at short intervals, this is a good idea anyway
- works for TLS?
 - this is trickier, have to bypass platform TLS trust
- no paths?
 - reliance on many CAs not common anyway ...
- new fed management processes/tools
 - may come, in InCommon, with SAML 2.0 support

- many/most feds may still use CAs
- many peers may just offer keys
 - ie, refuse to get new cert to establish relationship
- implying feds may need to handle both
- more future
 - dynamic discovery, dynamic establishment
ala OpenID
 - reputation management
 - will these things involve CAs?