Feds, PKIs, and Center

CAMP
Tempe, February 2006

RL “Bob” Morgan,
University of Washington and Internet2
Support organizational requirements for management of access to resources

- more resources
- more variety of resources
- more types of access
- more kinds of accessing parties
- more compliance drivers
- more threats, external and internal

... with acceptable risk, at acceptable cost
And that Internet thing?

Supports ubiquitous universal connectivity
... as permitted by policy, as needed for utility choices to limit connectivity *by design* will always lose eventually
so today, all new work is in frameworks that can support lots of ways to do it
"Federation"

uses SAML protocol for signon to web apps
user signon uses IdP-defined methods, usually pw
supports sending of user attributes for authz purposes

"PKI"

uses X.509 certs for authentication, object signing
uses SSL for protocol security
supports identity, non-repudiation

Not as different as you might think ...
SAML deployments use PK methods to identify and secure communication among components

How much can/should a SAML deployment use PKI methods to support its security?

meaning: full modern path validation names in certs vs names in SAML metadata

Shib lets you choose ...

put keys right in metadata, validate directly
put CAs in metadata, use PKI
but limited path validation in current code base
"PKI is more secure"

how it's kinda true

if SAML IdP uses passwords, passwords are sharable, stealable

SAML browser profile signon not as strong as key-based SSL client authentication

how it's not so true

private keys stealable too

SAML IdP can use PKI for user signon

PKI doesn't imply strong identity proofing, etc

PKI cost can inspire insecure shortcuts
"Feds do authz better"

how it's kinda true

SAML has attribute support designed in
standard SSL authn doesn't support attributes

how it's not so true

many PKI-based Grid systems support user attributes
via attribute certs or short-term attr-decorated ID certs
SAML products don't all provide good attribute support
attributes are not the entirety of authz ...
"PKI supports more apps"

how it's kinda true
   SAML only well-defined for web browser signon
   PKI supports many protocols via SSL, also does doc signing, wireless authn etc

how it's not so true
   browser increasingly dominant, capable (eg AJAX)
   many apps (eg IMAP) don't do client certs in practice
   some PKI aspects, eg bridge-based path validation, not supported across many products/platforms
"Feds support privacy better"

how it's kinda true

  SAML assertions can use generated-on-the-fly identifiers (or none at all if just user attrs)

  long-term certs have often-used identifiers

how it's not so true

  Grid-style attribute methods can avoid distribution of long-term identifiers in certs too

  advanced crypto methods can provide even stronger privacy properties
Basic organizational activity is identifying participating parties
   naming, vetting, assigning keys,
   identifying policies, contacts, responsibilities

Both benefit from
   identifying technology standards, supported apps
   operational support
   legal/policy frameworks
   comprehensively supporting a community

Is technology really a defining factor for community?
We are in the early days of supporting Internet-scale identity

many technologies being invented, standardized now

technology-centric structures (feds, bridged PKIs) must adapt or be left behind

some examples ...
Layered technology enhancing XML/SOAP/WSDL

Security components:

- **WS-Security**: adding sec properties to SOAP messages, including X.509, Kerberos, SAML profiles
- **WS-SecurityPolicy**: expressing endpoint policies to support flexible, adaptable implementations
- **WS-SecureConversation**: reinventing SSL in SOAP
- **WS-Federation**: "passive" profile just like SAML for browsers (supported in Shib), "active" profile for SOAP signon
- **WS-Trust**: ...
"User-centric identity"

See http://www.identitygang.org/ for much info

Motivated by

"Web 2.0", composition of services, blogosphere
people creating their identities on the Internet
identities that are not linked to big organizations
every blogger their own "provider" and relying party
"identity" not just userid or address, but buddy list,
photos, portfolio, reputation, etc

Many systems/protocols defined and built
SxIP, OpenID, Passel, LID, XRI/XDI, YADIS, ...
"Identity metasystem"

Proposal from Microsoft (Kim Cameron)
- influenced by user-centric principles
- "backplane" for many ID systems, or at least formats
- WS-Trust protocol as universal authn protocol
- Security Token Services translate among tokens

InfoCard
- implementation of metasystem client in Win Vista
- make user and service identities visible, editable
- new approach to web signon
InfoCard example
Other cool stuff

Liberty Alliance

WS-Framework for building identity-based services
alternative to WS-*, perhaps more practical
may be basis of further Shib/SAML work

Credentica (Stefan Brands) crypto technology

authn/z, e-cash with many advanced properties
for privacy, verifiability, etc

One-time passwords

OATH standard for SecurID-like things
mobile phone support etc
PKI bridging is well-understood, deployments happening

actual operational use, code to use it still in flux

SAML-based interfederation?

we already know it has to happen, eg InCommon and US E-Auth, eg many Euro federations
do we know how it will work? not yet
end-to-end vs intermediated arguments
is there least-common-denominator for practices?
transitivity question
All fits together?

Sure.
If we want it to.