Welcome

Acknowledgments and thanks
Security Acronymy: then and now
What’s working
What’s proving hard
Acknowledgments

NIH and NIST – Peter Alterman, Tim Polk and Bill Burr
NSF – Early Adopters and NSF Middleware Initiative
Internet2 Membership
PKI Labs, PKI Advisory Board, Neal McBurnett
Program Committee and Sean Smith
Security Acronymy circa 1998

PKI
X.500
X.509
CRL
RSA
PGP
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI</td>
<td>GXA</td>
</tr>
<tr>
<td>X.500</td>
<td>Liberty</td>
</tr>
<tr>
<td>X.509</td>
<td>Magic Carpet</td>
</tr>
<tr>
<td>CRL</td>
<td>SAML</td>
</tr>
<tr>
<td>OCSP</td>
<td>Shibboleth</td>
</tr>
<tr>
<td>LDAP</td>
<td>XML</td>
</tr>
<tr>
<td>RSA</td>
<td>HEBCA</td>
</tr>
<tr>
<td>PGP</td>
<td>FBCA</td>
</tr>
<tr>
<td>XKMS</td>
<td></td>
</tr>
<tr>
<td>SPKI</td>
<td></td>
</tr>
</tbody>
</table>
Security Acronymy circa 2002

E-authentication
9-11-01
OGSA
GSS
E-SIGN
E-LOCK
ACES
CAM
DAVE
Observations

I was really ignorant in 1998
This is proving really hard
There are a lot more approaches, if only because there are lots more needs
Partitioning the problem space may be better than the unified solution
What’s working

At the core, the math of PKI remains extremely elegant
The standards, protocols and processes of PKI are open
PKI attracts really smart people
What’s proving hard

Scaling: virtual organizations, federations, bridged hierarchies
Trust: collaborative versus legal
Integrating security and privacy
Mechanics: mobility, archiving, key escrow, identity
Authorization: role based versus atomic rights
Reconciling humans and lawyers
Interrealm Trust Structures

Federated administration
- basic bilateral (origins and targets in web services)
- complex bilateral (videoconferencing with external MCU’s, digital rights management with external rights holders)
- multilateral

Hierarchies
- may assert stronger or more formal trust
- requires bridges and policy mappings to connect hierarchies
- appear larger scale

Virtual organizations
- Grids, digital library consortiums, Internet2 VideoCommons, etc.
- Share real resources among a sparse set of users
- Requirements for authentication and authorization, resource discovery, etc need to leverage federated and hierarchical infrastructures.
The Continuum of Trust

Collaborative trust at one end…

- can I videoconference with you?
- you can look at my calendar
- You can join this computer science workgroup and edit this computing code
- Students in course Physics 201 @ Brown can access this on-line sensor
- Members of the UWash community can access this licensed resource

Legal trust at the other end…

- Sign this document, and guarantee that what was signed was what I saw
- Encrypt this file and save it
- Identify yourself to this high security area
Dimensions of the Trust Continuum

**Collaborative trust**
- **handshake**
- consequences of breaking trust
- more political (ostracism, shame, etc.)
- fluid (additions and deletions frequent)
- shorter term
- structures tend to clubs and federations
- privacy issues more user-based

**Legal trust**
- **contractual**
- consequences of breaking trust
- more financial (liabilities, fines and penalties, indemnification, etc.)
- more static (legal process time frames)
- longer term (justify the overhead)
- tends to hierarchies and bridges
- privacy issues more laws and rules
Applications and their user community must decide where their requirements fit on the trust continuum.

Some apps can only be done at one end of the continuum, and that might suggest a particular technical approach.

Many applications fit somewhere in the middle and the user communities (those that trust each other) need to select an approach that works for them.
Integrating Security and Privacy

Balance between weak identity, strong identity, and attribute-based access (without identity)

Balance between privacy and accountability – keeping the identity known only within the security domain
Reconciling Humans and Lawyers

Non-repudiation has had a very high bar set…

Human nature has been “refined” over a long time

We tend to talk globally, think locally and act inconsistently…
Conference Outcomes

Refine our understandings of security
Cross-pollinate PKI research
Identify experiments that should be conducted