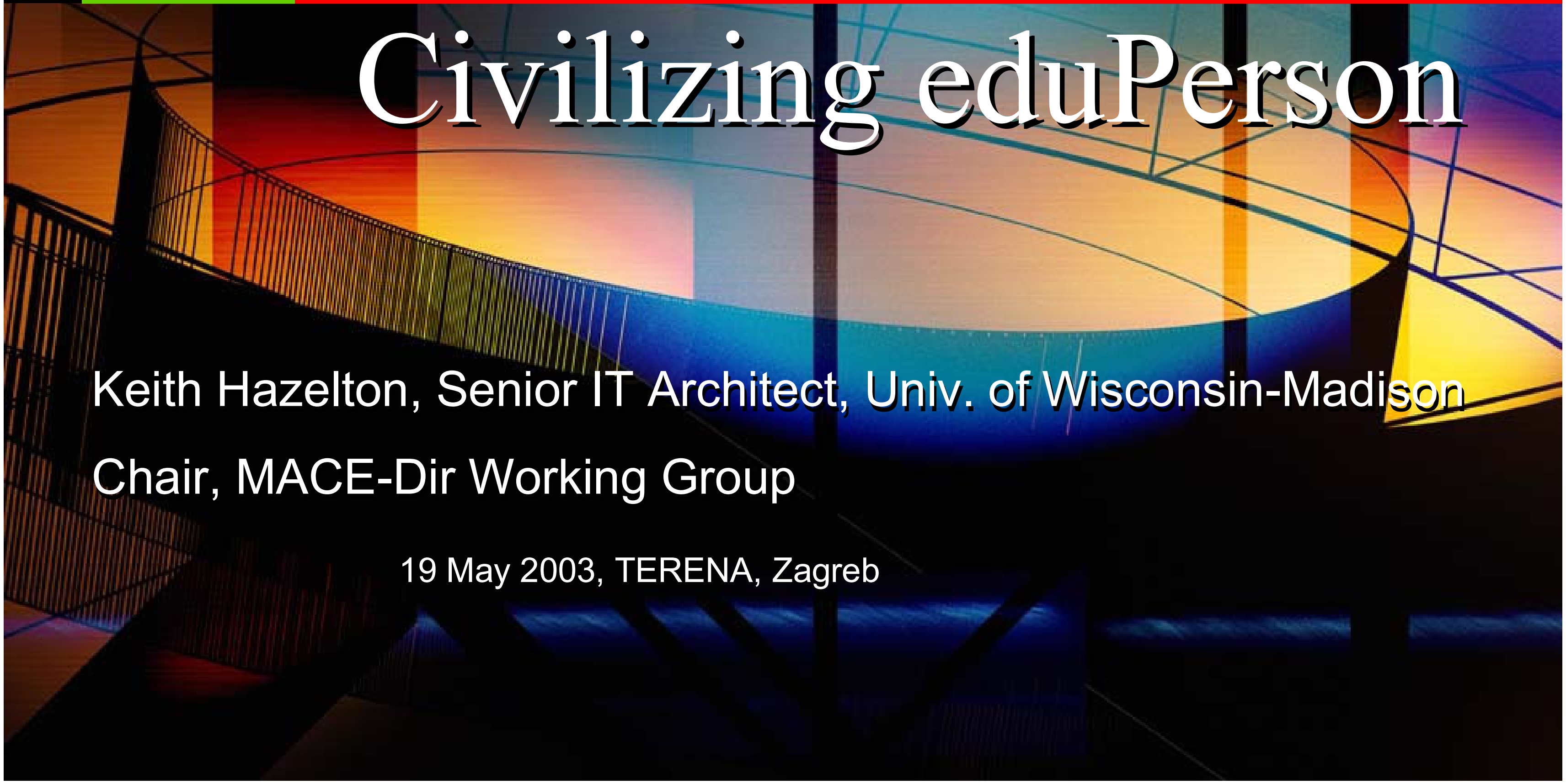

Civilizing eduPerson

Keith Hazelton, Senior IT Architect, Univ. of Wisconsin-Madison

Chair, MACE-Dir Working Group

19 May 2003, TERENA, Zagreb

Civilizing eduPerson: TOPICS

- Collaboration on schema work
- Reflections on European schema developments
- Trends in Internet2 schema and directories

Collaboration on Schema Work

- Person schema activities flourish
  - norEduPerson
  - funetEduPerson
  - swissEduPerson
  - DEEP survey questions on schema needs
  - &, of course, eduPerson
  - & further afield, WALAP activity in Australia
  - …& interest from East Asia heard at last JGN conference

Collaboration on Schema Work

- What to work toward?
- (In order of increasing difficulty and decreasing probability of success)
  - Agreement on a list of interesting attributes
  - Common syntax and semantics across schema for given attribute type
    - A kind of inter-federation diplomatic activity
  - Agreement on inclusion in a standard schema
    - eduPerson?
    - Next release of X.520?
    - Other candidates?
  - Processes for ongoing schema coordination
- Even common syntax & semantics would boost interoperability in attribute mapping

Collaboration on Schema Work

- How to do the work?
- Internet2 may be able to offer to host a concentrated series of conference calls or other virtual working sessions
  - Over six weeks or so
  - Scheduled to accommodate European & US (one set of calls)
  - …and Pacific -- US (a second, parallel set of calls)
- Charter would be to tackle the identified work items
  - Time permitting, move on to organizational object schema
- If successful, followons on Dir -- AuthN/Z links possible
- Let’s discuss all this in the days ahead…

Reflections on European schema developments

- *De Profundis*, or Lessons from the DEEP Survey
  - 6 of 8 eduPerson attributes considered “needed” by majority of respondents
    - 5 eP attributes by 13 or more of the 18 respondents
    - Affiliation and organizational place attrs. “won”
  - …But extensions needed, too
    - Mail for org object classes
    - Sensitive attributes like gender and birthdate and national ID number
    - Let’s talk!

Reflections on European schema developments

- Only half the respondents of the DEEP survey saw need for eduPersonEntitlement
- In US, this entitlement attribute is finding growing use controlling access to licensed resources under Shibboleth
  - Values are URIs (URL or URN)
  - URN:MACE: prefixed values proliferating after acceptance by IETF and upcoming registration with IANA
  - Gives way to make values unique in the entitlement namespace without elaborate registry mechanism

Reflections on European schema developments

- Deep survey revealed need for account and PKI object classes and attributes
- Largely untouched by edu* efforts of Internet2 MACE
- But important to ALL of us
- Also see value in the Gietz and Chadwick approaches to getting parsed X.509 certificate contents into our enterprise directories

Reflections on European schema developments

- Deep survey respondents nominated any number of attributes to carry unique identifiers
- eduPersonPrincipalName is the only one in current class
- Worth pondering how any of these would be used inter-domain (if they are)
- Many unsolved problems in federated identity management space bear on these issues

Reflections on European schema developments

- Privacy support attributes proposed in survey
- MACE-Dir discussions, too
  - Starting with collecting “communty practices”
  - Another area for Euro-US collaborative work

Reflections on European schema developments

- Schema registry project considered extremely valuable by Internet2
  - As a discovery tool
  - As a communication tool
  - As a possible Ur-Registration Authority for schema
  - As a protective measure against uncontrolled wheel re-invention

Trends in Internet2 schema and directory work

- eduPersonScopedAffiliation
  - Driven by Shibboleth needs
  - Syntax like eduPersonPrincipalName
    - student@brown.edu
    - alum@duke.edu
    - subscriber@nytimes.com (!?!)
  - Raises problems about who is authorized to assert what
    - An “inter-realm metadirectory function”
    - A field full of ratholes and land mines…

Trends in Internet2 schema and directory work

- Cautious and stringently limited expansion of controlled vocabulary for eduPersonAffiliation
  - prospective
  - parent
- …and maybe no more than that
- There's value in local attribute with more values
- And value in agreeing across institutions on syntax & semantics; but maybe not a single shared attribute
- Brings us full circle back to collaborative discussions…

Civilizing eduPerson

- Q & A