Identity and Access Management

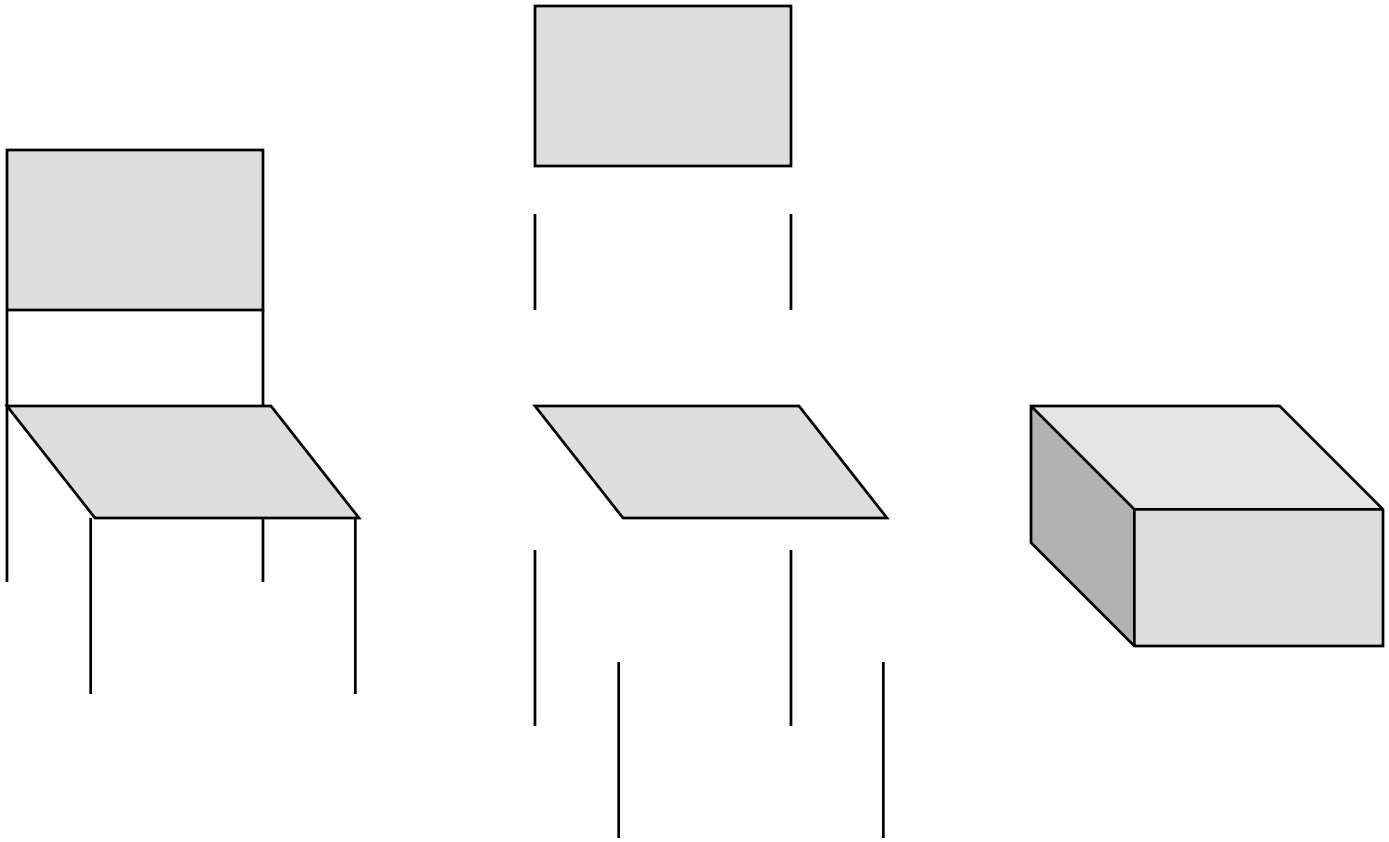
IT Support Community Event

July 31, 2002

Objectives

- Present “identity first” access management w/ rationale
- Discuss impacts to access provisioning
- Present ITS’ proposed direction
- Introduce sponsored identity
- Present future possibilities through federated identities
- Open discussion: how are your needs and university needs best met?

Identity (Buddha)



Courtesy Rob Blakley, IBM Tivoli Software

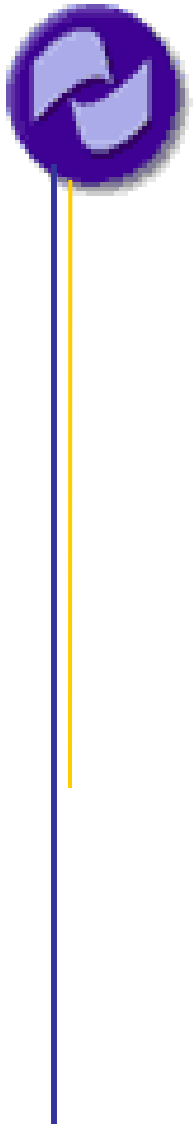
Identity (John Locke)

- "… the identity of the same *man* consists… in nothing but a participation of the same continued life, by constantly fleeting particles of matter, in succession vitally united to the same organized body.

- "Any substance vitally united to the present thinking being is a part of that very same self which now is; anything united to it by a consciousness of former actions, makes also a part of the same self, which is the same both then and now. *Person*, as I take it, is the name for this self."

- "… as to this point of being the same self, it matters not whether this present self be made up of the same or other substances - I being as much concerned, and as justly accountable for any action that was done a thousand years since, appropriated to me now by this self-consciousness, as I am for what I did the last moment. In this personal identity is founded all the right and justice of reward and punishment."

Courtesy Rob Blakley, IBM Tivoli Software



Huh?

Identity (CU)

- cuEduPerson Directory Entry derived from HR or SIS data.
- Consistent across campus (and University).
- Establishes university affiliation(s) and thus role(s) and entitlements.

“Identity First” Access Management

Means:

You must have an Identity in the Campus Enterprise Directory in order to be granted access to any services.

Your Identity establishes your role and entitlements to receive services.

Why?

Benefit to You:

- Consistent representation of you (with controllable access to specific information) across the University System reduces your headaches when dealing with multiple touch points (and reduces touch points).
- Ability to predict your needs and automate (or streamline) the University's ability to meet them, especially as your role changes.

Benefit to the University:

- Assures appropriate use of resources by those who funded them.
- Allows us to satisfy legal and licensing requirements to control access of services to appropriately affiliated people.
- Enables standard and consistent mechanisms for managing access to IT resources, reducing implementation times and increasing security.

Access Management / Provisioning

Ideal:

Role Based Access Controls (RBAC) using Identity attributes and extended Identity attributes.

Access Management = Managing Identity Attributes

Reality:

Provisioning local accounts in systems.

Access Management / Provisioning

Ideal:

Role Based Access Controls (RBAC) using Identity attributes and extended Identity attributes.

Access Management = Managing Identity Attributes

Reality:

Provisioning local accounts in systems.

BUT: Provision using Identity (consistency) and attach local account to Identity (extend Identity).

Access Management += Provisioning Based on Identity Attributes

ITS Direction

Identity First Access Management

- Provision accounts on ITS systems using Enterprise Directory Identity.
- Implement RBAC authorization mechanisms and/or use Identity attributes. E.g. Dial-up modem access being specifically enabled based on affiliation rather than being side-effect of getting IdentiKey.
- Streamline provisioning processes and provide more self-help (web) functions, particularly for faculty/staff.
- Build infrastructure that supports/enables both Web Access Management and local account provisioning based on Identity (started with the Enterprise Directory).
- Champion use of this infrastructure and Identity First Access Management campus-wide.

Establishing a University Identity

- PeopleSoft HR and SIS are primary systems of record.
- This means that a person *must* have a PeopleSoft or SIS entry *before* they can get accounts on ITS systems!

Sponsored Identities

- Recognizing need for non-student, non-employee access to CU resources.
- Not second-class citizens. Have Identity in Directory with associated attributes (which are used for access management).
- THUS: Must have “strong” affiliation with University (visiting researcher OK, mother-in-law not OK).
- Must be sponsored by “officially” affiliated faculty or staff (who is accountable), through a designated Sponsor Administrator (perhaps).
- Have finite relationship with the University.

Sponsored Identities (cont.)

Examples of Sponsored Identities:

	Regent	Summer Conference Attendee
Entitlement Level	High (e-mail, shell accounts, etc).	Low (Res. Hall lab access only)
Duration	4 years	2 weeks

Sponsored Identities (cont.)

Scenario:

Sponsored affiliate becomes “official” affiliate.

- Requires that sponsored Identity be reconciled with HR or SIS data.
- Emphasizes importance of complete and accurate data for sponsored Identities.

Status

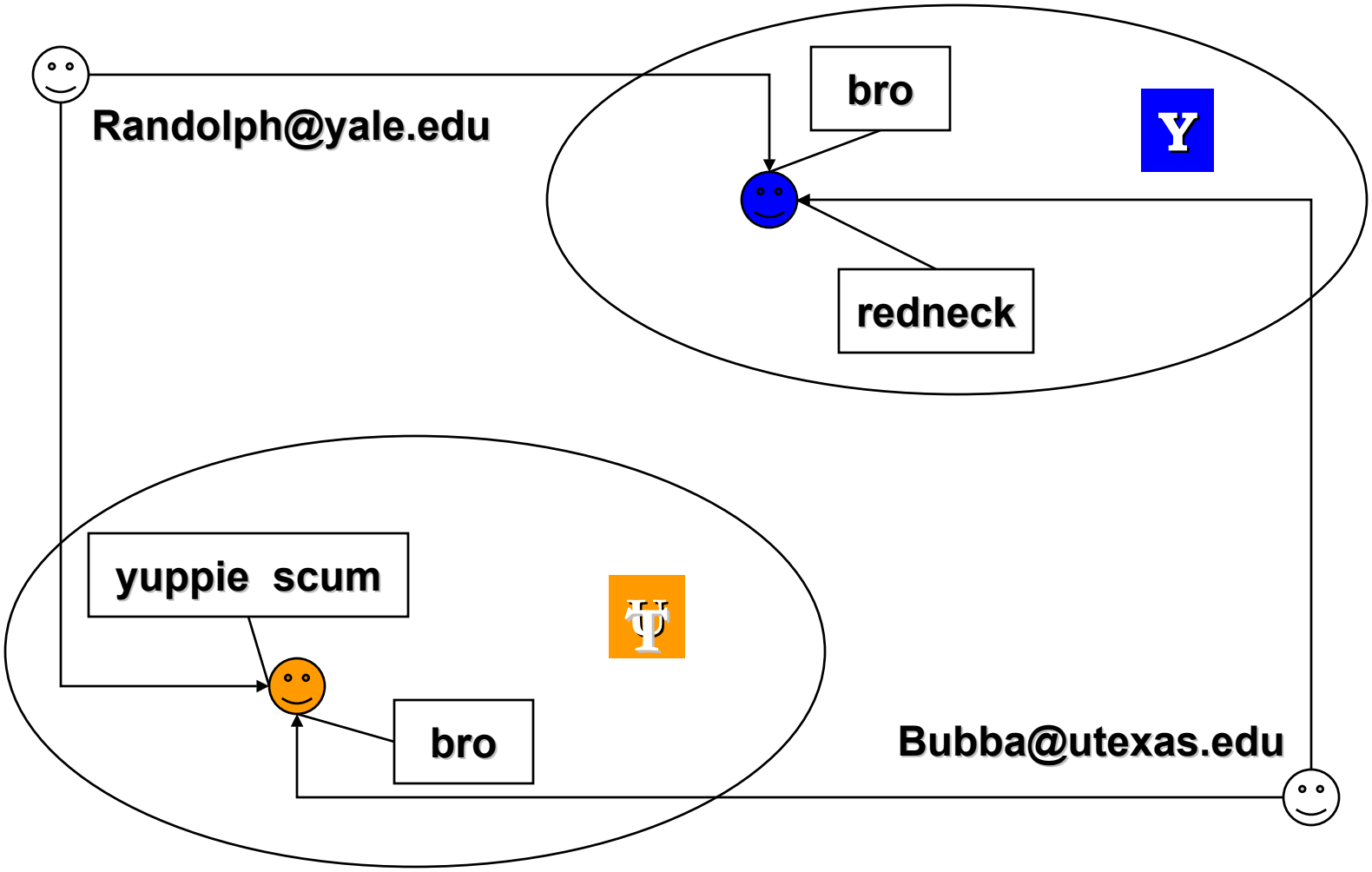
- Directory Services Project
  www.colorado.edu/Committees/DirectoryServices
- Sponsored Identity Support in Registry
- ITS Provisioning Initiative
- ITSPI Component of the Campus IT Strategic Plan

Identity Federation

"Authenticate locally, act globally."

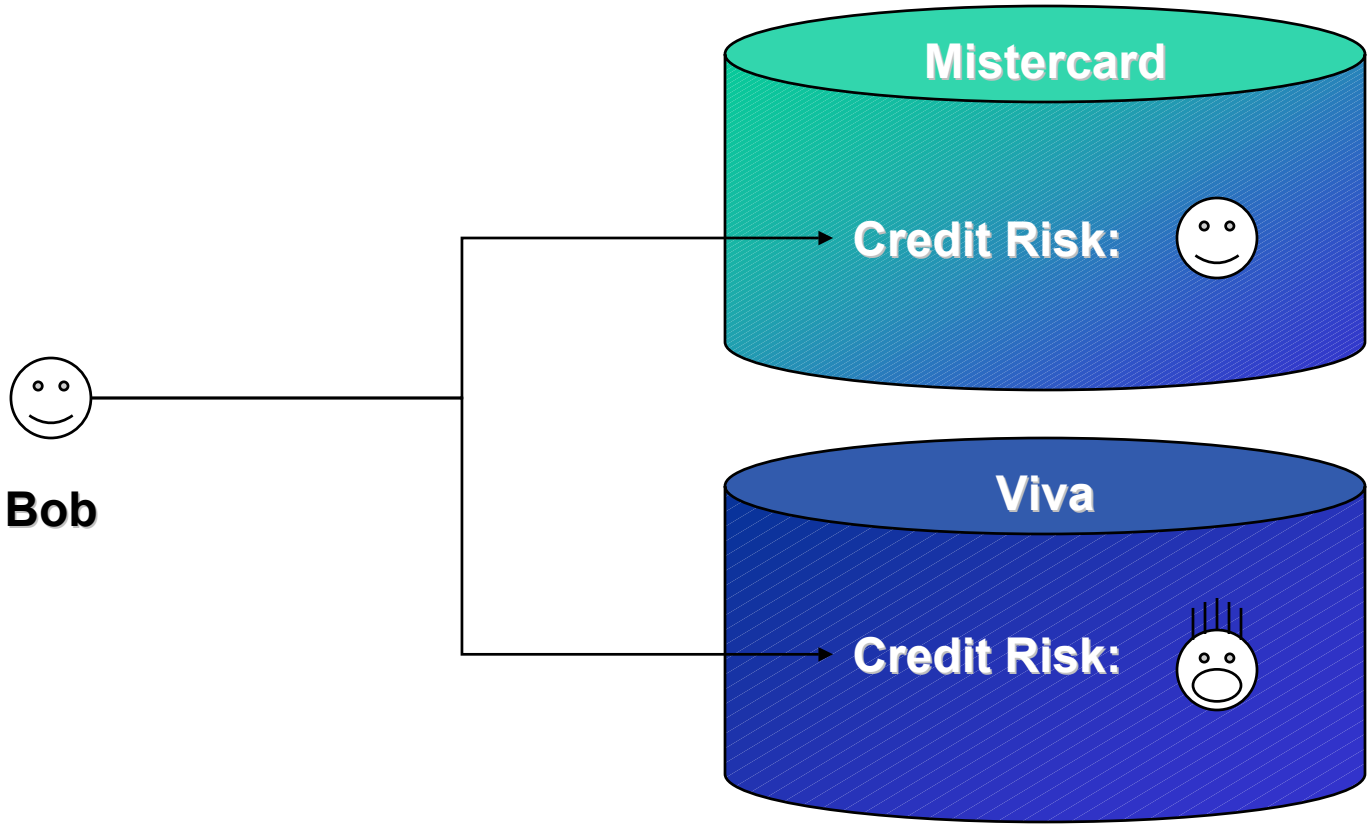
- Liberty Alliance Project (http://www.projectliberty.org/)
- Internet2 Shibboleth (http://middleware.internet2.edu/shibboleth/)

The Essence of Federation (1)



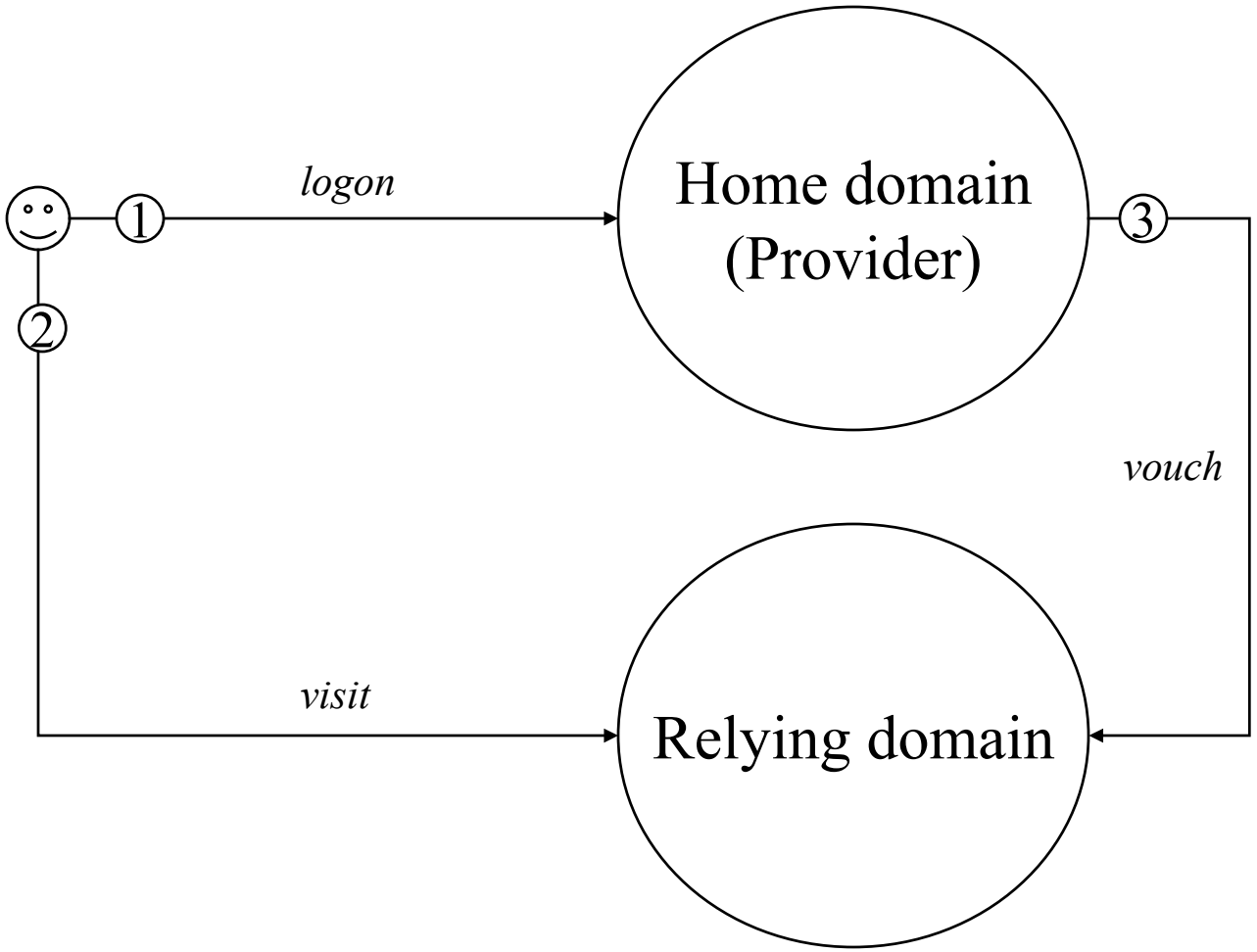
Courtesy Rob Blakley, IBM Tivoli Software

The Essence of Federation (2)



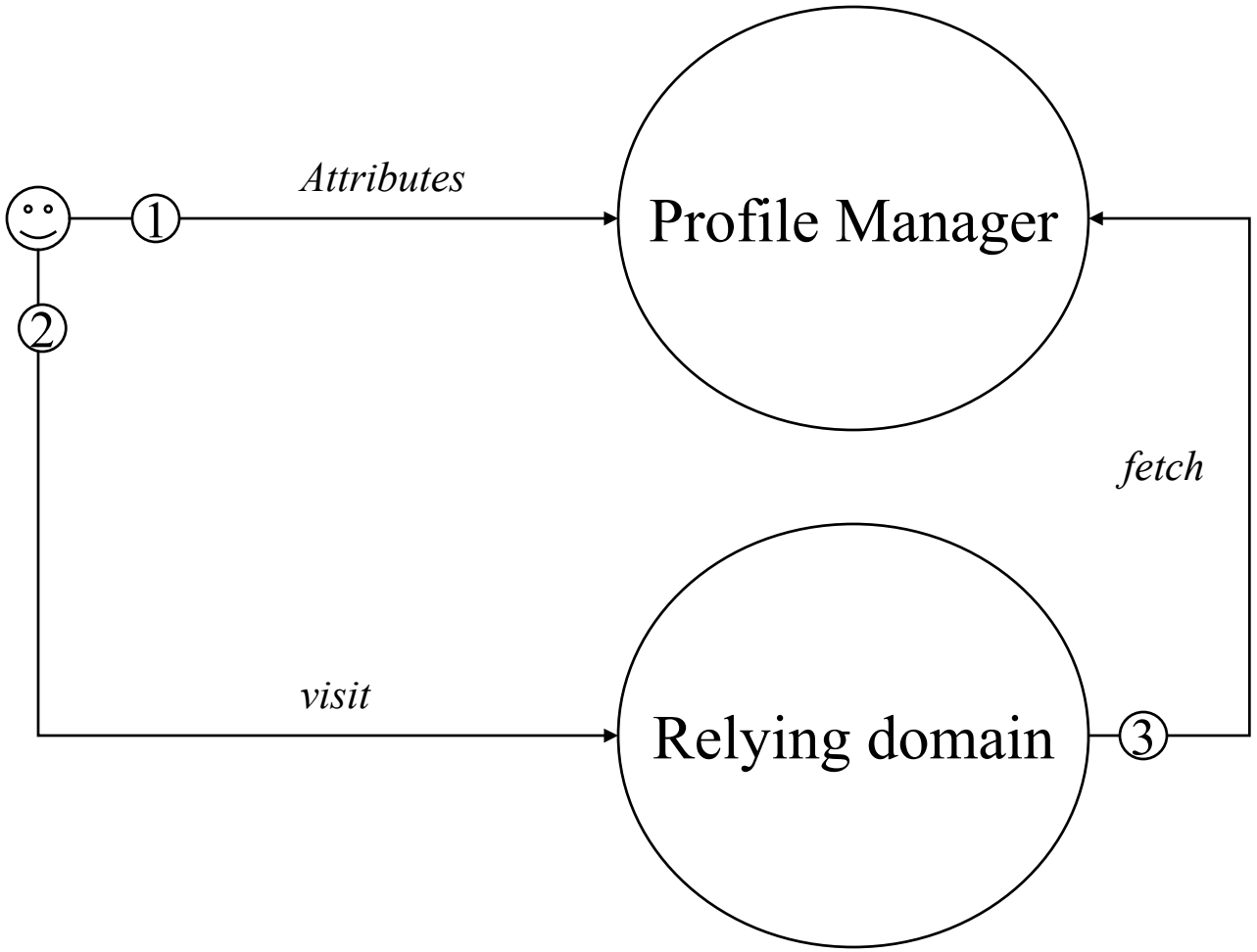
Courtesy Rob Blakley, IBM Tivoli Software

Federation Mechanism: Federated Authentication



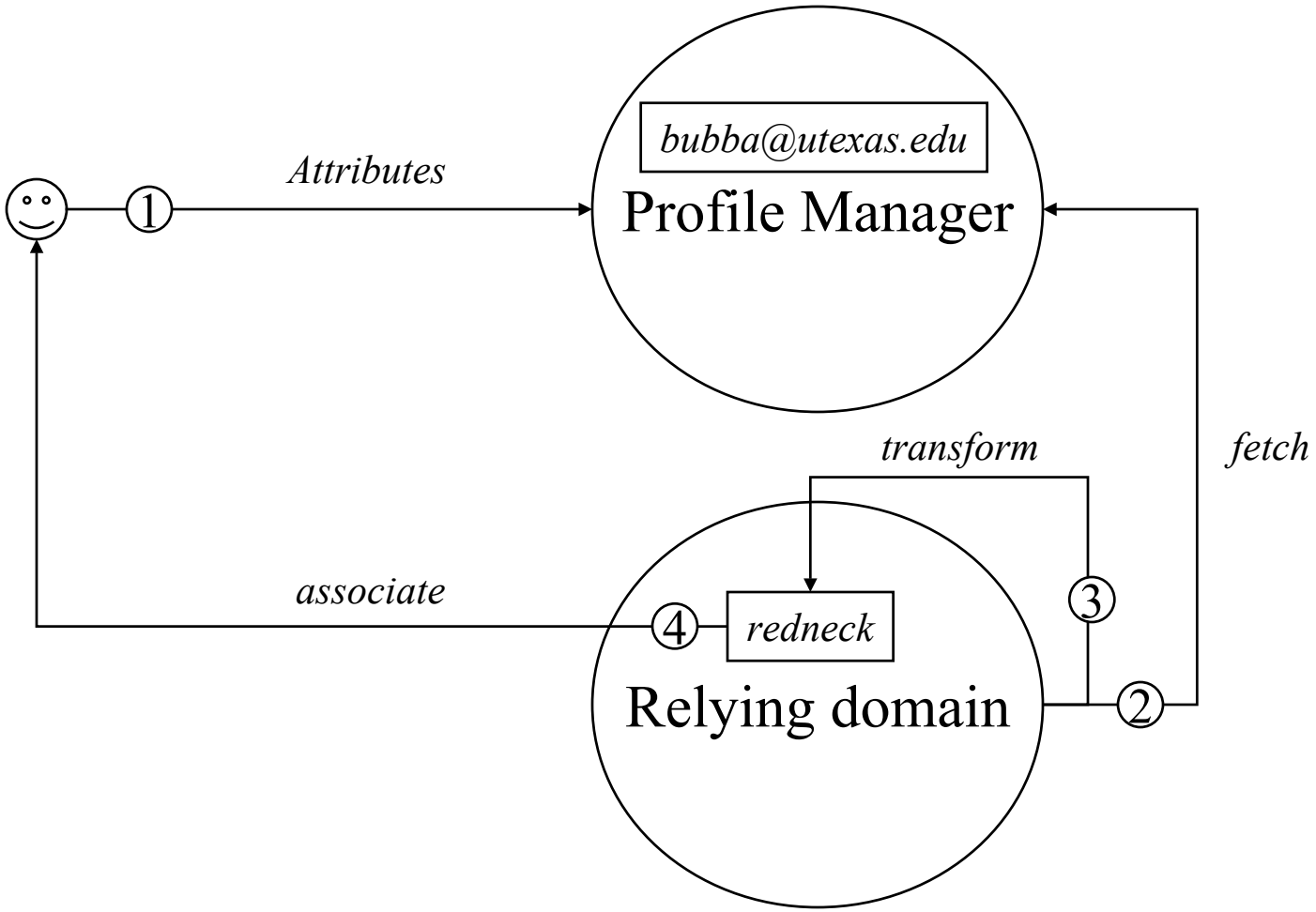
Courtesy Rob Blakley, IBM Tivoli Software

Federation Mechanism: Attribute Assertion



Courtesy Rob Blakley, IBM Tivoli Software

Federation Mechanism: Attribute Transformation



Courtesy Rob Blakley, IBM Tivoli Software