DIX BOF
Digital Identity eXchange

65th IETF, Dallas
March 21st 2006

Welcome and Introductions

- Chair – Scott Hollenbeck,
  shollenbeck@verisign.com
- Chair – John Merrells,
  merrells@sxip.com

- Wiki – http://dixs.org
- Jabber – dix@rooms.jabber.ietf.org

Housekeeping

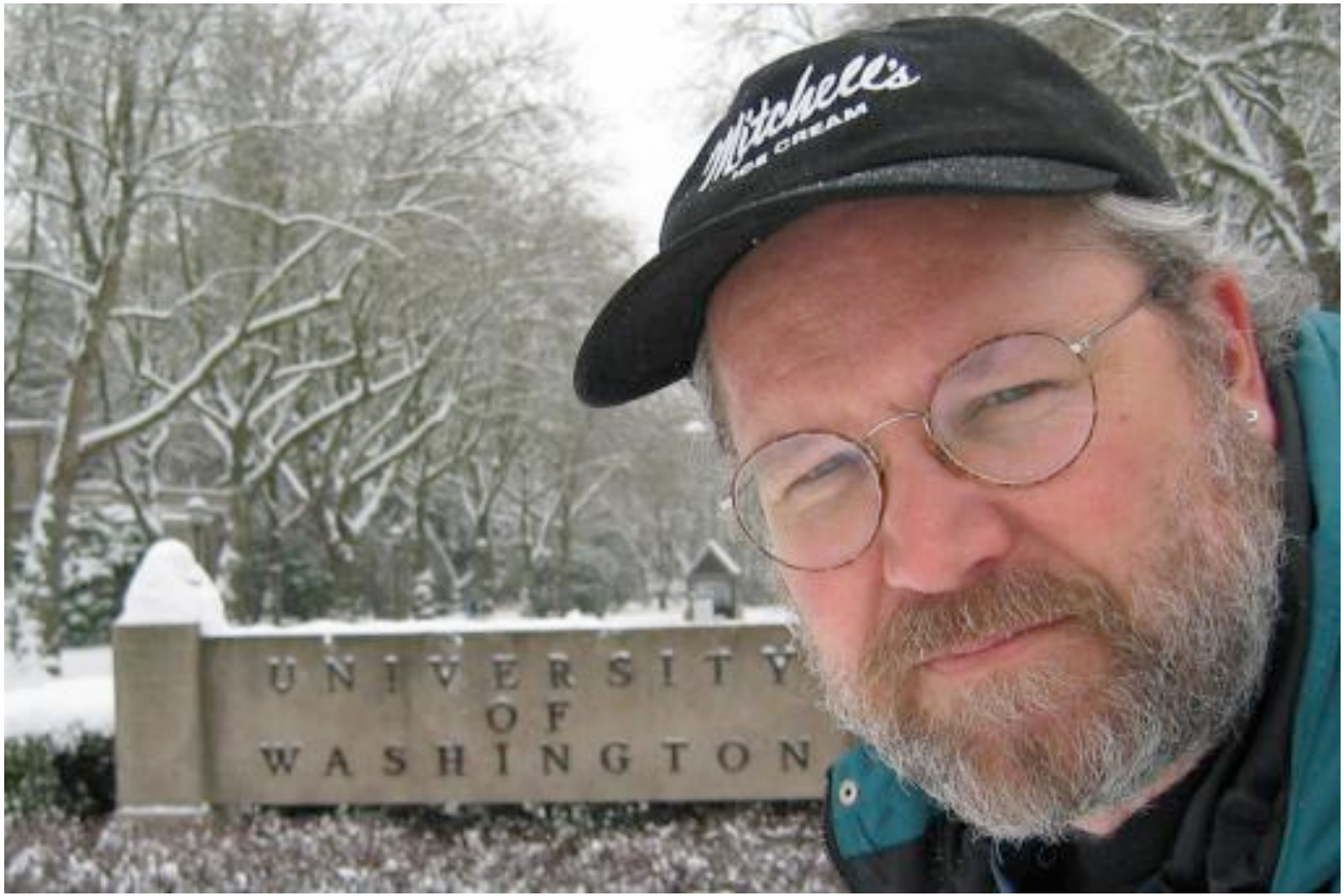
- Use Microphones for those on the audio channel
- State your name clearly for the scribe
- Discussion points after each agenda item
- We need scribes…

- Wiki – http://dixs.org
- Jabber – dix@rooms.jabber.ietf.org

Agenda

Time	Topic
10	Agenda Bashing
20	Problem / Goals / Benefits
30	Scope
20	Requirements
20	Architectural Options / Related Work
10	draft-merrells-dix-00.txt (dmd0)
40	Discussion

Scene Setting



Scene Setting

- “Enterprise Identity Management” (IdM)
  - Access control for resources
  - Leverages many IETF technologies
    - LDAP, Kerberos, PKIX, TLS
  - Includes
    - Authentication
    - Roles

Scene Setting

- Web Authentication
  - 1996 survey - 12+ solutions
  - Why this interest?
    - Enterprise Web Applications
    - Required: SSO, Minimal password exposure, browser based
    - Web is easy to hack on
  - So, many open-source, in-house, and commercial solutions, even leveraging IdM

Scene Setting

- Today's Web
  - Millions of blogs, homepages, etc
    - Represent online lives
    - Other's interact with them
    - But: Who's on my site?
      (For expression… rather than control)
    - Required: SSO and Information Exchange
      (But, no enterprise IdM system)

Scene Setting

- New Goals
  - User-Centric
  - Widely Deployable
  - Good Enough Security
- Web-scale ubiquity to be compelling

Scene Setting

- Questions
  - Is new technology required?
    Or new usage of existing technology required?
  - What are the user requirements?
  - What are the barriers to wide adoption?
  - Different than ‘Enterprise’ technology?
    Or just part of the whole spectrum?

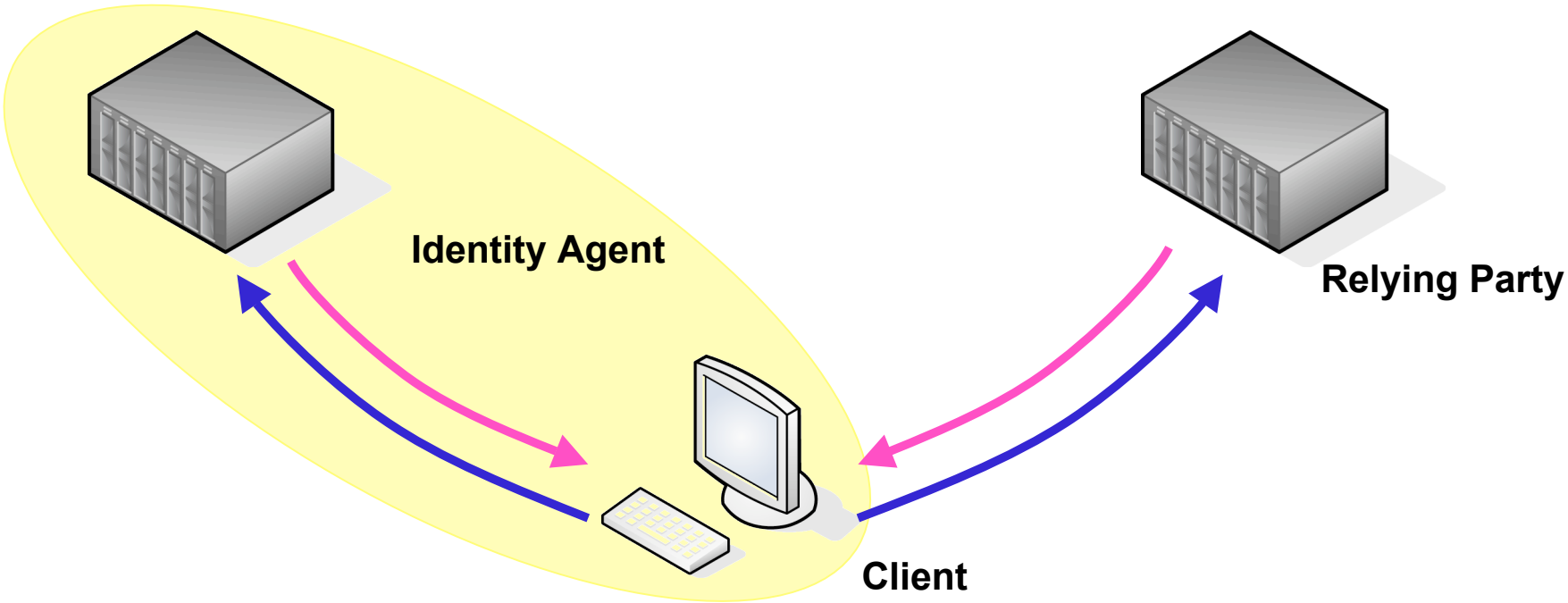
Definitions

- Digital Identity Exchange
- Identity Agent
- Relying Party
- Claim
- Digital Subject

Definitions

- **Digital Identity Exchange**
  - “The transmission of digital representation of a set of Claims made by one Party about itself or another Digital Subject, to one or more other Parties.”
  - RL ‘Bob’ Morgan, 14th March 2006, DIX Mailing List

Definitions



Definitions

- **Claim**
  - An assertion made by a Claimant of the value or values of one or more Identity Attributes of a Digital Subject, typically an assertion which is disputed or in doubt.

Definitions

- **Digital Subject**
  - An Entity represented or existing in the digital realm which is being described or dealt with.

Problem Statement

- “The Internet is host to many online information sources and services. There is a growing demand for users to identify, and provide information about themselves. Users bear the burden of managing their own authentication materials and repeatedly providing their identity information. Signing in to web pages and completing user registration forms is an example.”

Proposed Draft Charter
http://dixs.org/index.php/DIX_Charter

Problem Statement

- **For User**
  - Manage many Username/Passwords
  - Retyping same data into forms
- **For Service Operator**
  - Low conversion ratios
  - Data inaccuracy
  - Minimal data exchange

Example

- User goes to a web site
- User provides some information about themselves

Just complete the information below so that Amazon.com can recognize you.

New to Amazon.com? Register Below.

My name is:

My e-mail address:

Type it again:

My birthday is: Month Day **(optional)**

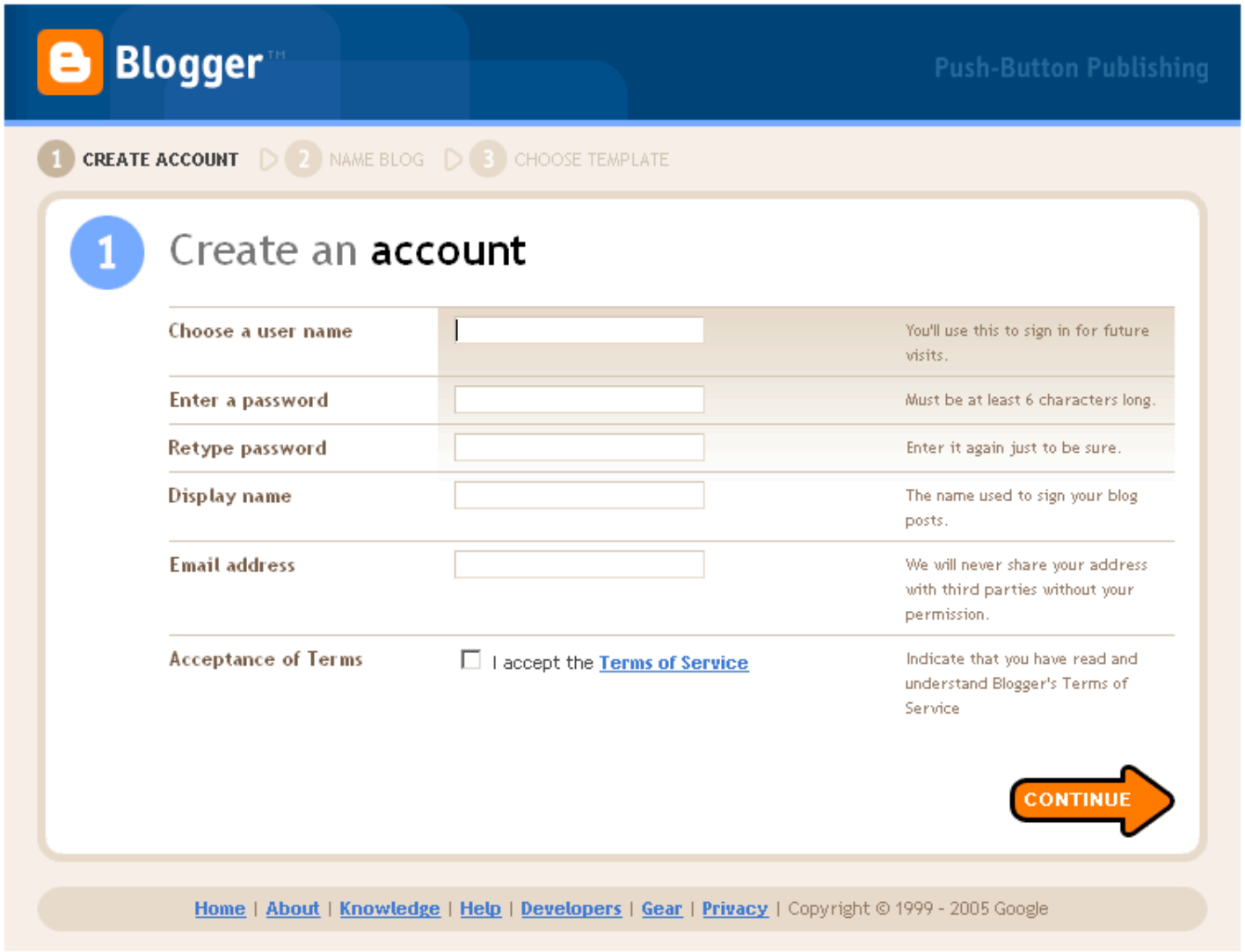
Protect your information with a password

This will be your only Amazon.com password.

Enter a new password:

Type it again:

Continue


Blogger™
Push-Button Publishing
1 CREATE ACCOUNT
2 NAME BLOG
3 CHOOSE TEMPLATE
1
Create an account
Choose a user name
You'll use this to sign in for future visits.
Enter a password
Must be at least 6 characters long.
Retype password
Enter it again just to be sure.
Display name
The name used to sign your blog posts.
Email address
We will never share your address with third parties without your permission.
Acceptance of Terms
I accept the Terms of Service
Indicate that you have read and understand Blogger's Terms of Service
CONTINUE
Home | About | Knowledge | Help | Developers | Gear | Privacy | Copyright © 1999 - 2005 Google

Register: Enter Information

Help

1 Enter Information 2. Choose User ID & Password 3. Check Your Email

If you want to bid or buy on eBay, you'll need to register first. It's easy and **free**.

First name

Last name

Street address

City

State
Select State

Zip code

Country
United States

Primary telephone
( ) - ext.:

Secondary telephone (Optional)
( ) - ext.:

Date of Birth
–Month– –Day– Year

Important: A valid email address is required to complete registration.

Email address

Examples: myname@yahoo.com, myname@example.com, etc.

Re-enter email address

Continue >

Expedia.ca
Now we're getting somewhere.

Welcome - Already a member? Sign in

home | flights | packages | hotels | cars | deals | activities | maps | business

User Guide | Site Map |

Create a new account

Start enjoying the same great deals, personal service, and secure purchases that millions of travellers have discovered. Learn more about Expedia.ca.

Create an account

Personal title:
-- Select from list --

First name: Middle name: (optional) Last name:

Tip: Make sure this name matches the traveller's passport or driver's licence to avoid travel delays.

User name: (4-30 characters)

Password: (6-30 characters)

Type password again:

Supply e-mail address

We'll use this address to confirm your travel purchases or notify you of a reservation change.

Current e-mail address:

☑ E-mail me travel deals, special offers, and information about my trips.

Sign up and continue using Expedia.ca

Note that account creation may take a minute or two.

Online bits

Your website:

Website name:

Do you use Instant Messaging?

AIM (AOL IM): **Yahoo! IM:**

MSN Messenger: **ICQ:**

Offline bits

Your Occupation:

Your Hometown:

City you live in now: **3 letter Airport Code:**

Country: (Need help finding yours?)

- Other
- Rather not say

- Open
- Rather not say

Your Birthday: Day Month Year

Describe Yourself...

(Some HTML is OK.)

LinkedIn

Join LinkedIn

Your privacy is our top concern.

We work hard to earn and keep your trust, so we adhere to the following principles to protect your privacy:

- We will never rent or sell your personal information to third parties for marketing purposes
- We will never share your contact information with another user, unless both of you choose to contact one another
- Any sensitive information that you provide will be secured with industry standard technology

LinkedIn sends updates about new features of interest to members no more than once a month. You may opt out of these updates at any time.

Joining LinkedIn only takes a moment.
Please enter the following information to create your account.

Basic Information:

First Name:

Last Name:

Email Address:

Password: 6 or more characters

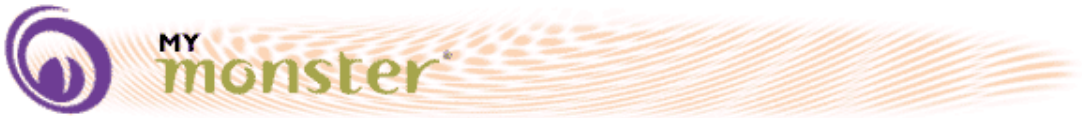
Re-enter Password:

Country: United States

ZIP or Postal Code: only your region will be public, not specific postal code

Professional Basics:

Status:
- ☐ I am currently employed:
  - Company/organization:
  - Title:
- ☐ I am a business owner:
  - Company/organization:
- ☐ I am a consultant or contractor
- ☐ I am currently looking for work
- ☐ I work independently
- ☐ I am currently a student:
  - Name of School:
  - Degree:
  - Graduation Year:



Create New My Monster Account

* Required Information

*First Name
*Last Name

*Home Address
Home Address
*City/Town
*Province — --- Select ---
*Postal Code
*Country — Canada
*Email Address

What is your email format preference? — HTML / Text

*Create a Username — Use between 4 and 20 letters and/or numbers
*Create a Password — Use between 4 and 20 letters and/or numbers
*Confirm Password

Password Question — --- Select ---
Your Answer

To help remember and protect your password, supply a personal ""hint"" by selecting a Password Question and answering it below.

Create a Screen Name — For chats, etc.

Automatically log in to Monster from this computer?
Not recommended if you are using a public computer.
Yes / No

*Relevant Work Experience — --Select--
*Career Level — --- Select ---
*Degree/Level Attained — --- Select ---

Submit Cancel

The New York Times
ON THE WEB

Already a Member? Log In

Registering for NYTimes.com is free and easy!

Registration provides instant access to everything you love about The New York Times and more.

Why Register? | Privacy Concerns | Cookies Information | FAQ's

Create an Account (Required)

Choose a Member ID:

Choose a Password: (Five character minimium)

Re-enter your Password:

Secret Question: --- Select One --- What's this?

Secret Answer:

E-Mail Address: Why do we need this?

NYTimes.com will only use this address with your permission.

☑ Remember my Member ID and password on this computer.

Tell Us About Yourself (Required)

Gender: ○ Male ○ Female

Year of Birth: (Click here if you are under 13)

ZIP Code:

Country of Residence: --- Select One ---

Household Income: --- Select One ---

Job Title: --- Select One ---

Industry: --- Select One ---

Technorati

Sign In | Help

Search

Keyword or URL

Become a Technorati Member

To join, just fill out this simple form. An asterisk (*) denotes required information.

First Name

Last Name

Email Address*

Pick a Username* Four characters or more. Will be public.

Choose a Password* Six characters or more.

Re-enter Password*

Year of Birth Under 18? Read our Minors Privacy statement.

Company Name

Zipcode

Country Select one ...

Do you have a blog? Yes No

I agree to abide by the Terms of Use.

I wish to subscribe to Technorati's email newsletter.

Please review our Privacy Policy for more information.

Join Technorati

travelocity

Home | Flights | Hotels | Cars/Rail | Vacations | Cruises | Last Minute Deals

Become a Member

Get a free membership with instant benefits.

- Access to Last Minute Deals and Real Deals newsletter.
- Fare change alerts with FareWatcher[SM].
- Security and Privacy. We don't sell or rent names. See the Travelocity Privacy Policy.

*=Required

1 Personal Information

Title:
*First Name:
Middle Name/Initial:
*Last Name:
*Zip/Postal Code:
*Country: United States

2 Log-In Information

Your e-mail address will be your log-in name. All trip-related communications will be sent to this address.

*E-Mail Address:
*Confirm E-Mail Address:
*Password:
*Confirm Password: Tips for selecting a password.

Type in a personal question / phrase / word that will help you remember your password in case you forget it.

Password Hint:

E-Mail Format: With graphics (HTML) Without graphics (Text)

Yes, send me the weekly Real Deals newsletter so I can be informed of the best airfare and travel deals just for me!

3 User Agreement

Becoming a member of Travelocity constitutes your acceptance of the terms of the Travelocity User Agreement.

MY YAHOO!

Yahoo! - Help

Already have an ID or a Yahoo! Mail address? Sign In.

Fields marked with an asterisk * are required.

Create Your Yahoo! ID

* First name:

* Last name:

* Preferred content: Yahoo! U.S.

* Gender: [Select]

* Yahoo! ID:

ID may consist of a-z, 0-9 and underscores.

* Password:

Six characters or more; capitalization matters!

* Re-type password:

Yahoo! Mail: Create my free Yahoo! email address.

Your address will be the ID you've chosen followed by @yahoo.com.

If You Forget Your Password...

* Security question: [Select a Question]

* Your answer:

Four characters or more. Make sure your answer is memorable for you but hard for others to guess!

* Birthday: [Select a Month] dd , yyyy

* ZIP/Postal code:

Alternate email:

Customizing Yahoo!

Industry: [Select Industry]

Title: [Select a Title]

Specialization: [Select a Specialization]

Proposed Goals

- Automate Digital Identity Exchange between User and Service
- Protect User's Privacy
- Minimize Barriers to Adoption

Benefits

- **For Users**
  - Convenient Digital Identity Exchange
  - Richer experience with Service
- **For Service Operators**
  - Increased quality and quantity of identity data
  - Higher conversion rates

Role & Scope of IETF

- Internet related problems
- “Above the wire and below the application”

- DIX is within IETF scope

Proposed DIX Scope

- In Scope
- Out of Scope
- In/Out of Scope?

- *Narrow, yet also ambitious.*

In Scope

- Digital Identity Exchange between User and Service
- HTTP/HTML Transport
- Browser based applications

Out of Scope

- Digital Identity Exchange between services
- Federating identifier namespaces
- Usage of digital certificates
- Claim schema and type system
- User authentication with Identity Agent

In/Out of Scope?

- SIP
- XMPP
- Non-browser based applications
- Third Party Claims

Scope Discussion?

Requirements

Seven Laws of Identity

1. User Control and Consent
2. Minimal Disclosure for Constrained Use
3. Justifiable Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human Interaction
7. Consistent Experience Across Contexts

Kim Cameron

http://www.identityblog.com/

Requirements – Digital Identity Exchange

- Move claims from agent to service
- Move claims from service to agent
- Unique identifier for User

Requirements - Privacy

- Unique Identifier for User
  - No central control
  - Opaque
  - Unidirectional (1:1)
  - Omni-directional (1:N)
  - Separation from Identity Agent
- Minimal disclosure

Requirements - Claim Schema

- Globally unique Identifier for Names
- Easily extended

Requirements - Adoption

- Nominal client footprint
- Minimal changes to Service
- Service can independently extend Claim Schema
- Leverage existing standards
- Ad hoc Service and Identity Agent relationship
- No more security than needed
  - Security Gradient

AD HOC From Here

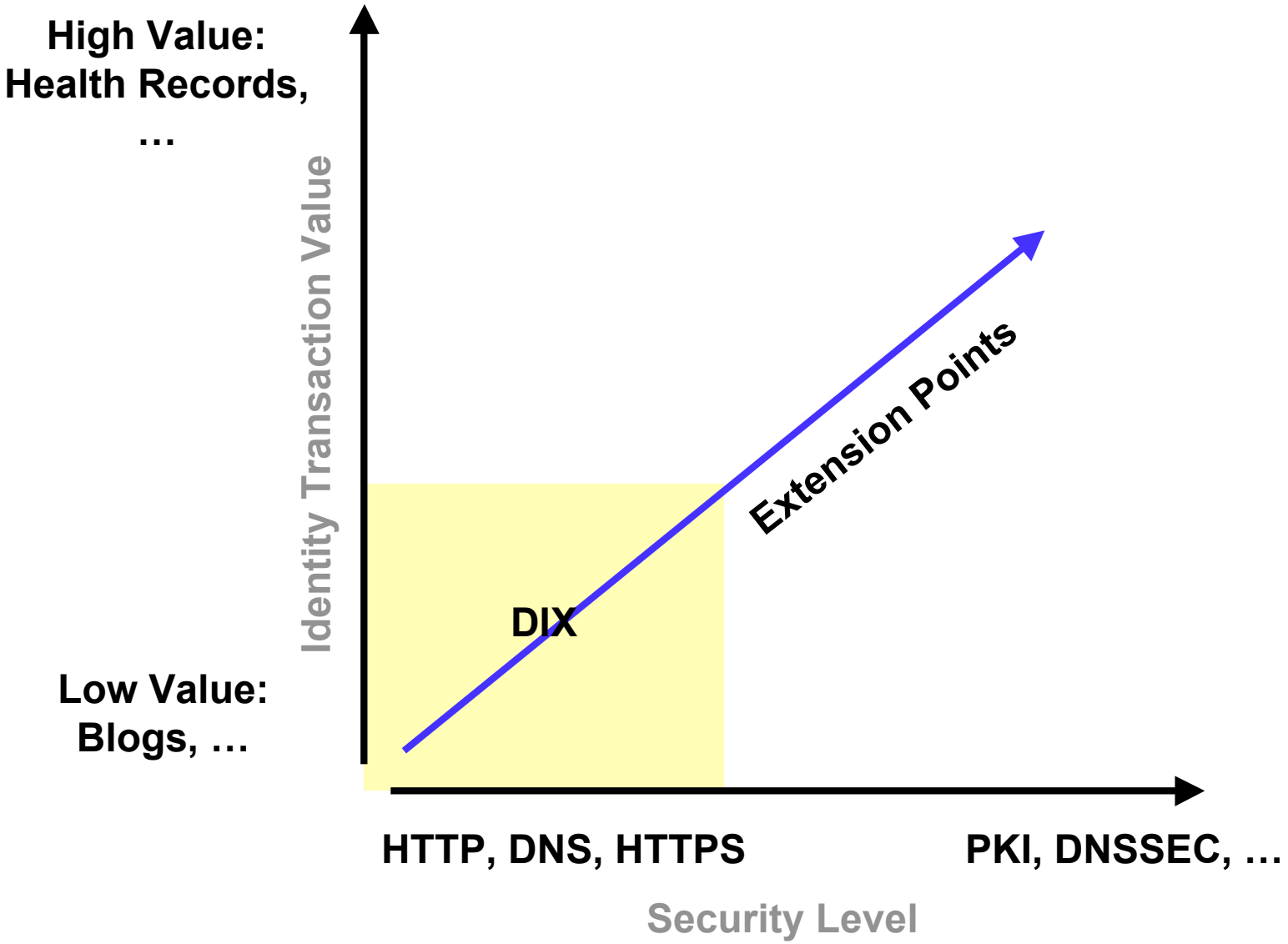
DIX - Problem Statement #2 ?

- Unified approach to self and authority stated claims (Bob)
- ‘Friendly’ Multiple Portable Unique Identifier for Users (Phil/Dick/Lisa)
- Simple and easy to deploy/adopt (Love)
- Peer-to-peer exchange of identity information (Bob)
- Privacy…
- Use Case: Blogosphere. Not satisfied by existing technology? (Phil)
- Internet scale for trust

DIX - Consensus Points ?

- BOF should go away - No
- Elliot's Dad problem: Multiple sites, multiple passwords. (PF: Restated as an Identifier problem?) - Yes
- E: Minimize dependent third parties. PHB: Deployment Costs. Know who the user is?
- JH: Reusing existing technology, where appropriate?
- PHB: Write requirements of Blogosphere Use Case? DC: 3-5 Use Cases, not addressed by other tech. - Yes. 7 ppl

Security Gradient - Example



Threat Analysis

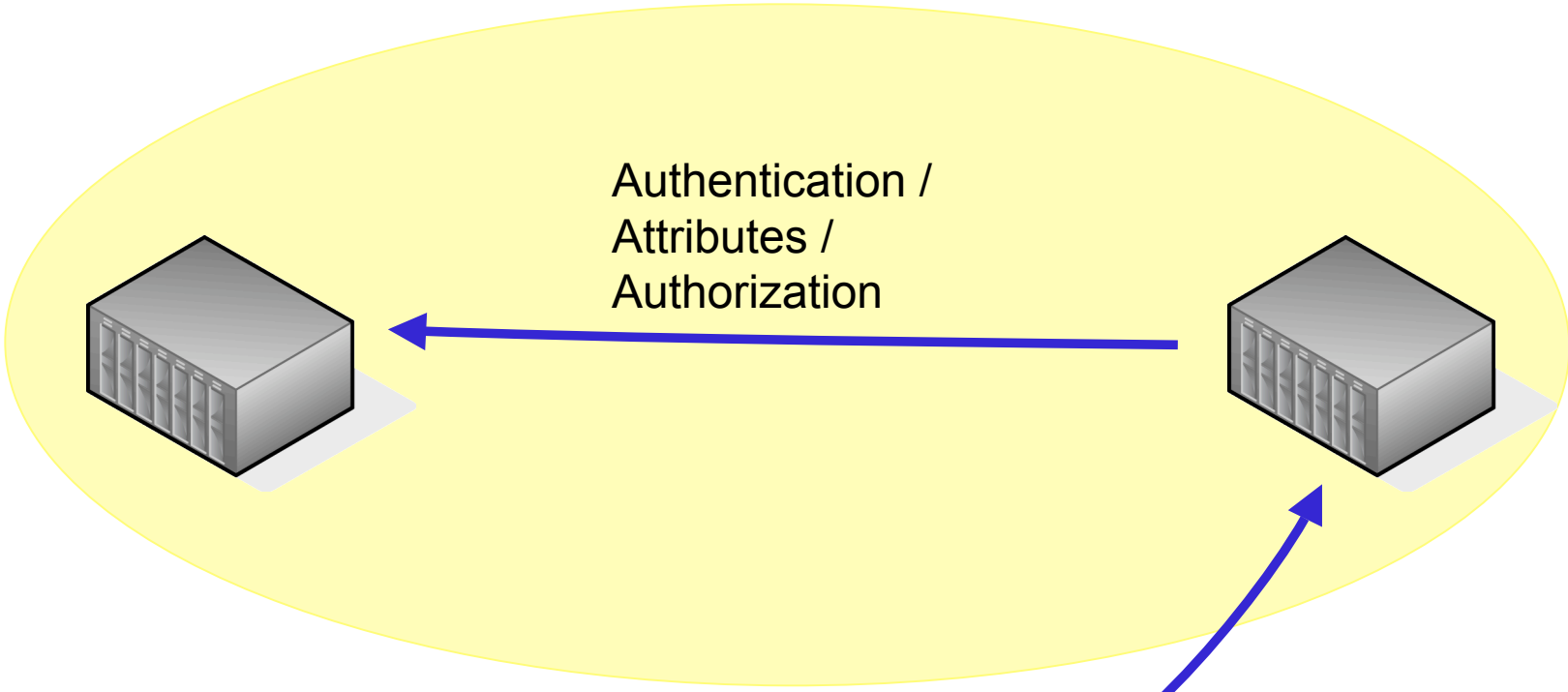
- Vulnerabilities and security limitations will need to be analyzed and well documented

Requirements Discussion?

Architectural Models

- Domain Centric
- Federation
- User-Centric

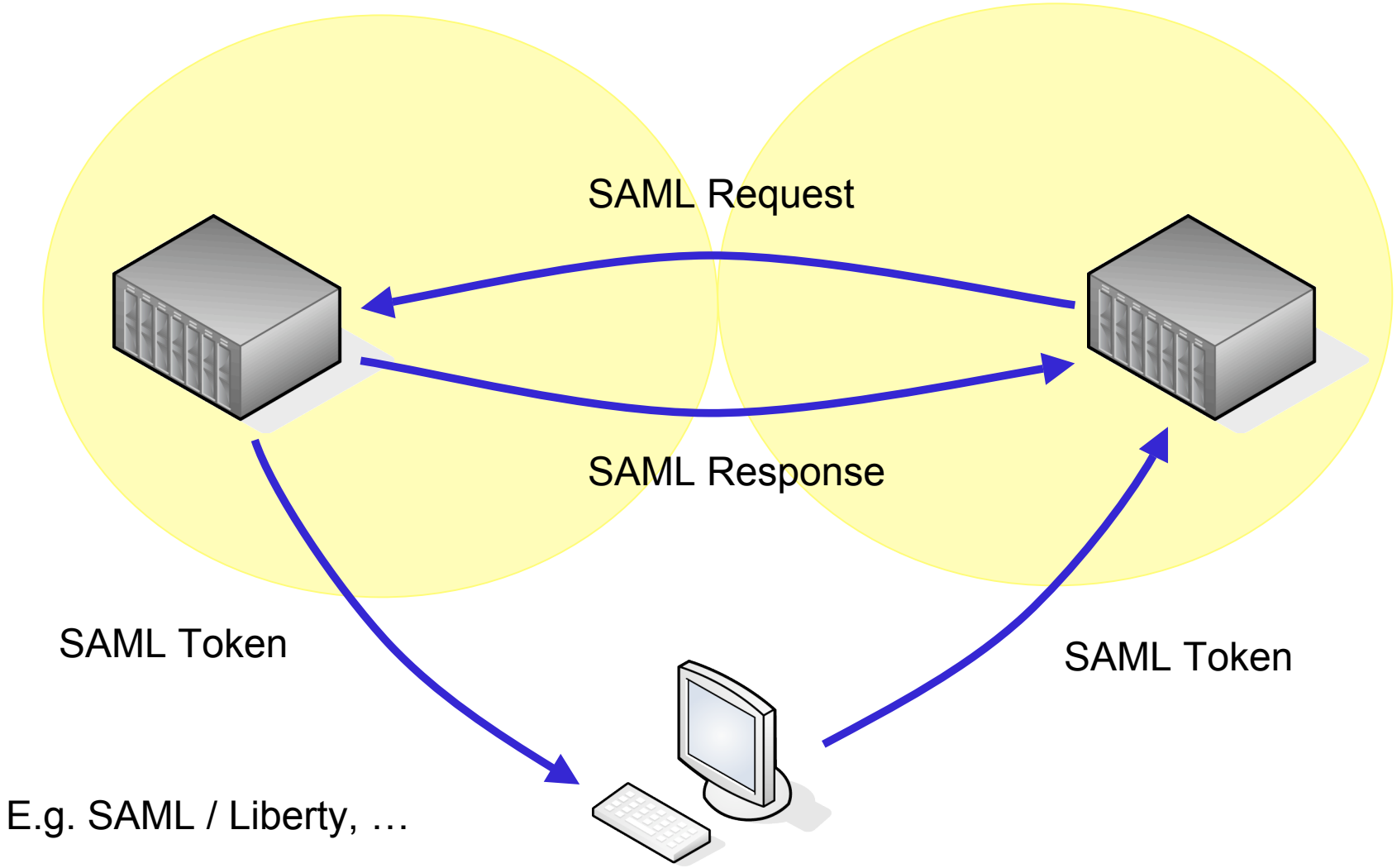
Domain Centric



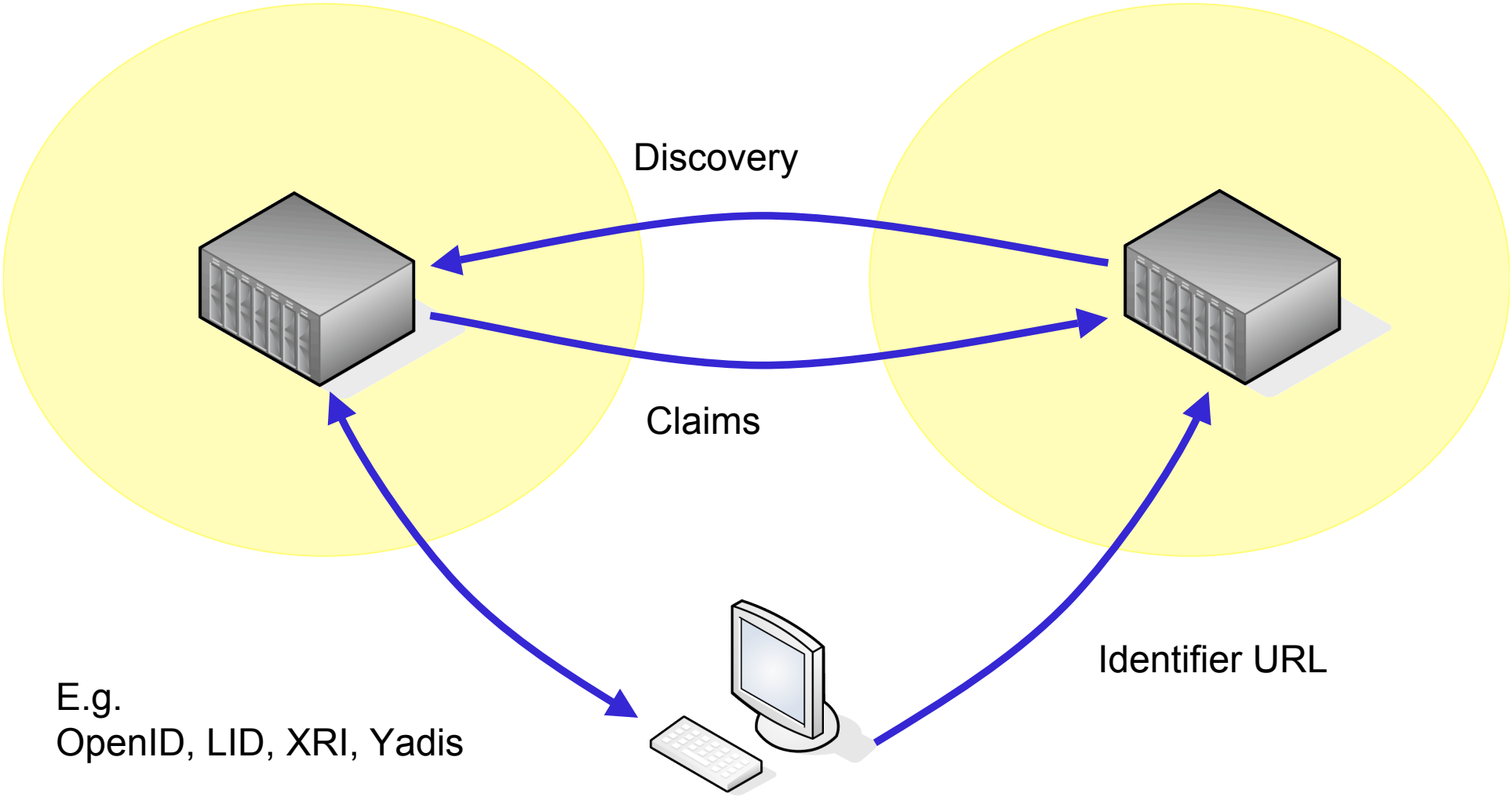
E.g. X.500, LDAP,
Kerberos, PKIX, TLS,
SASL, HTTP Basic/Digest,
…

Account
Credentials

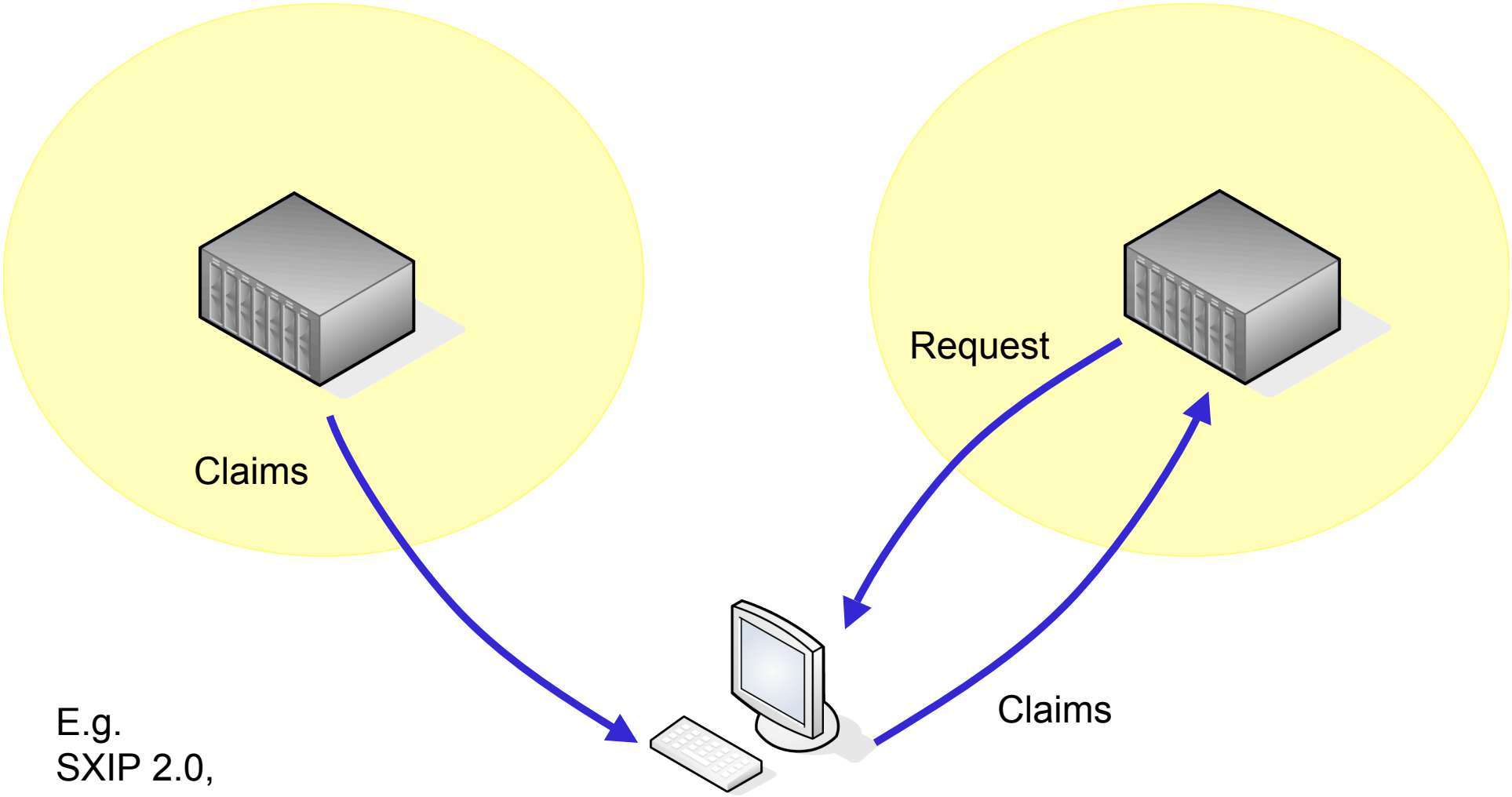
Federation


SAML Request
SAML Response
SAML Token
SAML Token
E.g. SAML / Liberty, …

Federation - Ad Hoc



User Centric



E.g.
SXIP 2.0,
WS-Trust / MetaSystem,
…