What is Federation
(and why should I care)?

Rob Crittenden, Red Hat, Inc.

rcritten@redhat.com

usenix LISA15

November 8–13, 2015 | Washington, D.C.
www.usenix.org/lisa15 #lisa15

Identity

- More than a login id
- You have many:
  - Work
  - Personal interests: sports, hobbies, etc.
  - Software

Federated Identity

- Portability of identity across domains
- Reduces administrative overhead of redundant information

The Parties

- Federation has three participants. I'm going to use SAML2 lingo:
  - Identity Provider (IdP)
  - Service Provider (SP)
  - End user

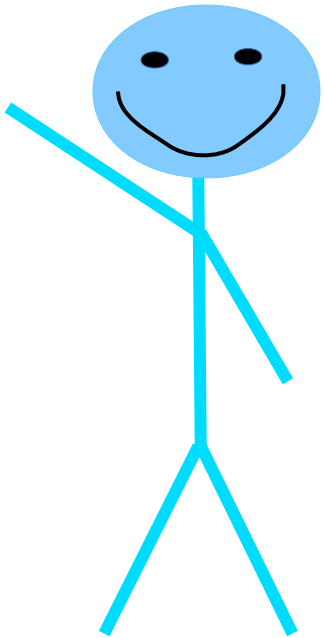
Identity Provider

- Trusted provider that manages identity information and provides authentication
- Can be part of your infrastructure or a trusted 3rd party

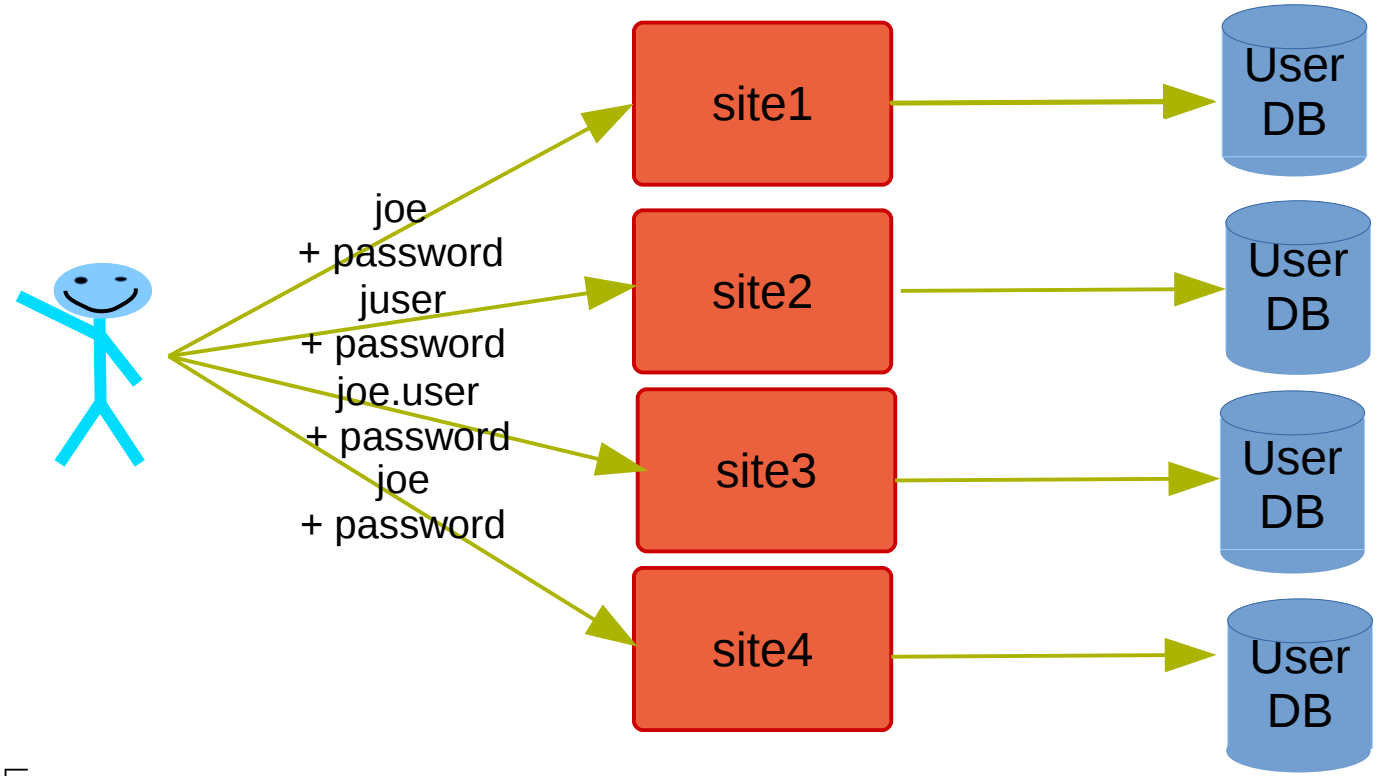
Service Provider

- A Web Server
- Relies on a Identity Provider for authentication
- Can be in or out of your control

Users



Typical Web Usage



The Problem?

- Multiple Passwords
  - Some almost certainly bad
  - Possible re-use
- Remembering which password goes where
- Reliance on each web site protecting its user database

A solution: Federation

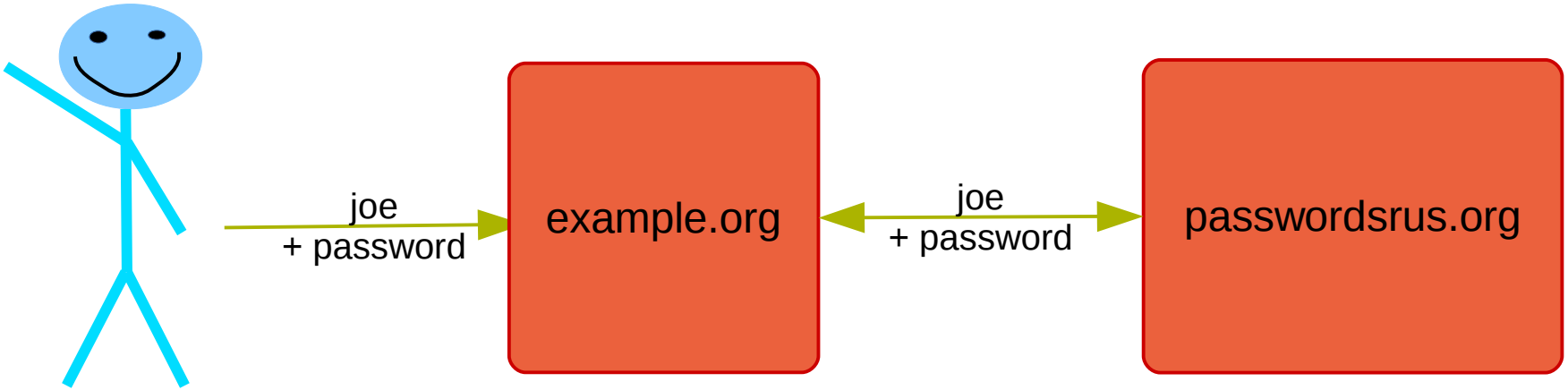
- Good for Users:
  - One account* to use everywhere
    - So one password, hopefully a good one
  - Rely on trusted 3rd party to protect passwords
- Good for Web Applications/SPs:
  - Can support additional authentication methods
  - Reduce administrative overhead
    - No user passwords to manage

Federation Highlights

- Trust a 3rd party to do the authentication
- Generally a web-based protocol over TLS
  - Doesn't always require a browser, e.g. rich mobile client
- Centralized or Decentralized
- Common protocols:
  - SAML, OpenID and OpenID Connect

Not Federation

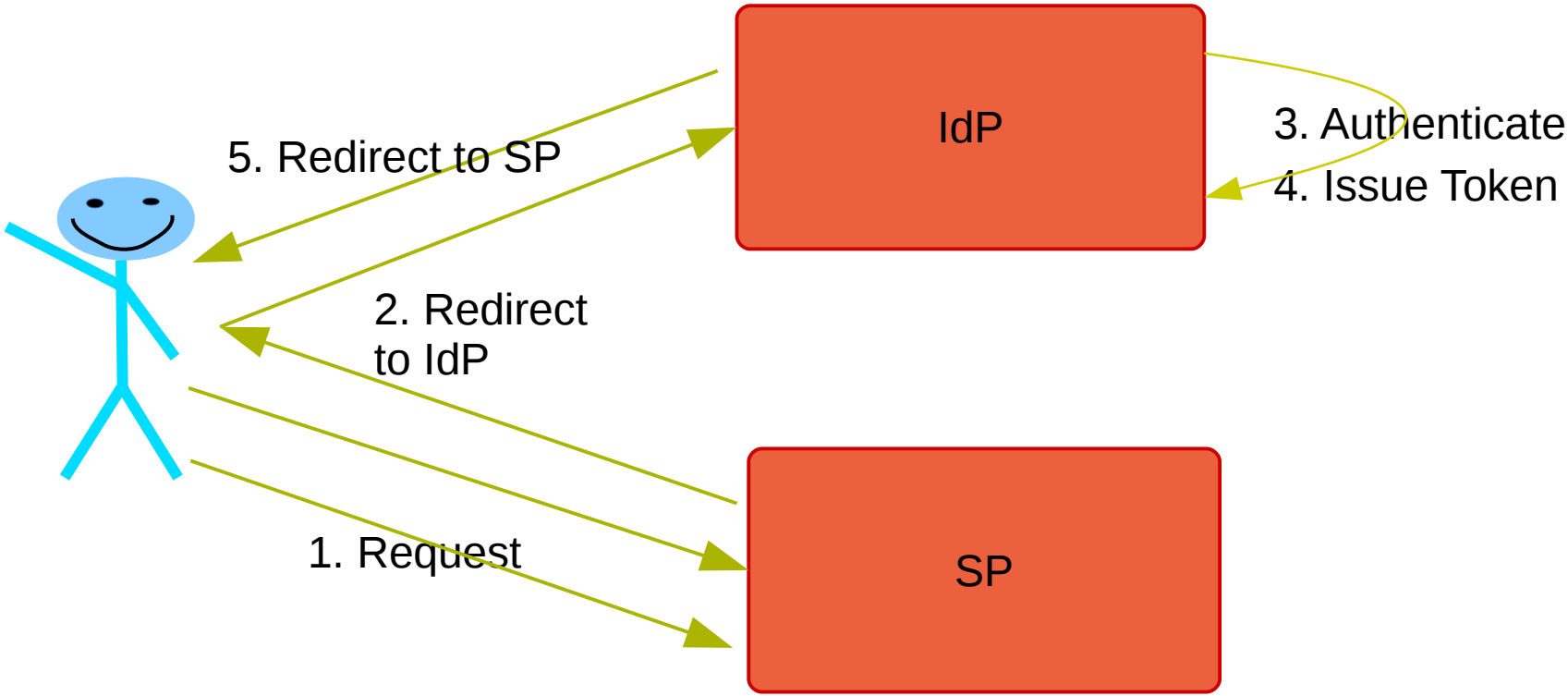
- No control of credentials



SAML 2.0

- Mature
- XML and SOAP over HTTPS
- Centralized: requires agreement between parties
  - Exchange of metadata and public keys
- Single sign on and Single logout

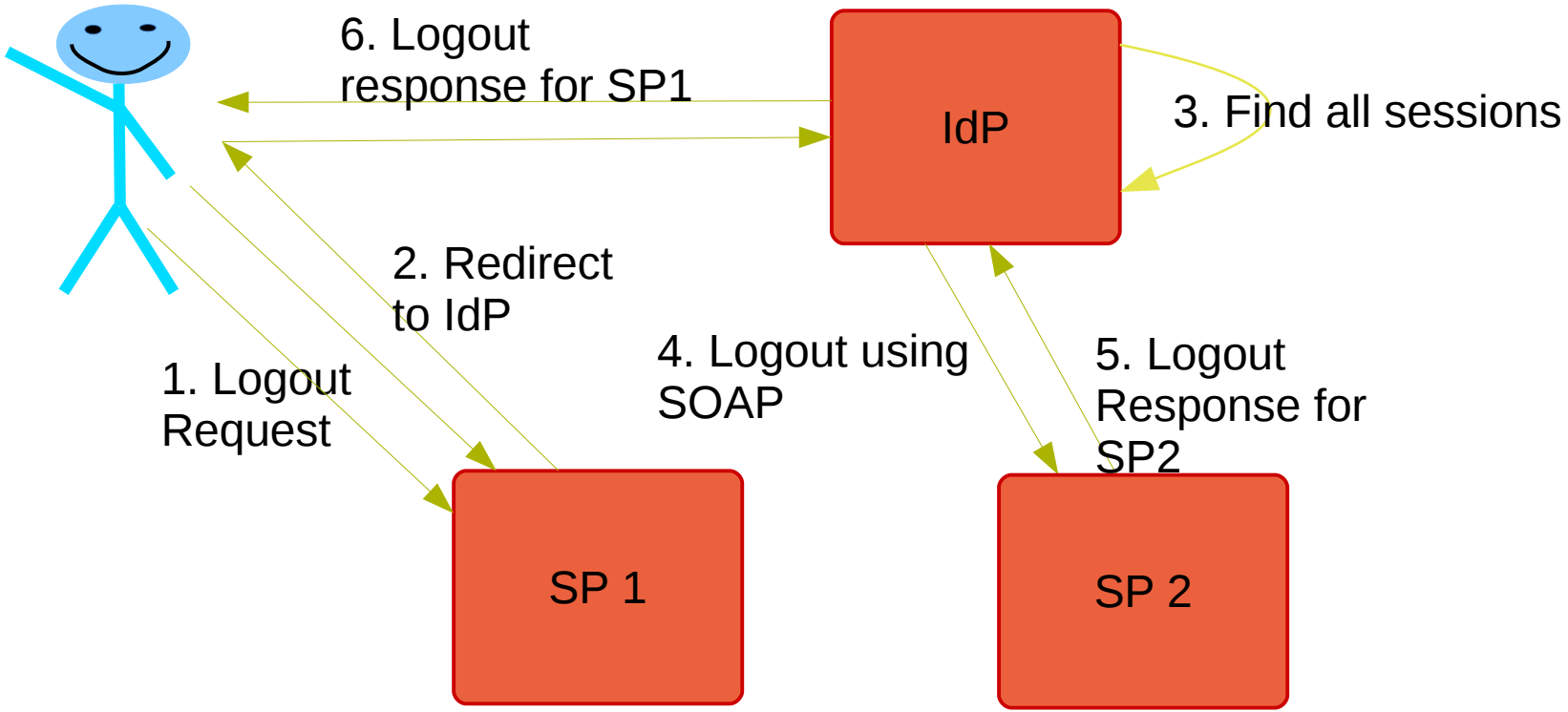
How does SAML login work?



SAML Assertions

- Authentication
  - NameID
- Attributes
- Authorization Decision
- Signed

SAML Single Logout



SAML Use Cases

- Typically Enterprise
- Single Sign On
- Employees at Acme, Inc can manage customer relationships at Salesforce using corporate identity
- Book airlines, hotels or cars

SAML Identity Providers

- Shibboleth
- Keycloak
- Ipsilon
- SimpleSAMLPHP
- OpenSSO

SAML Service Providers

- Shibboleth
- Keycloak
- mod_auth_mellon
- SimpleSAMLPHP
- OpenSSO

OpenID

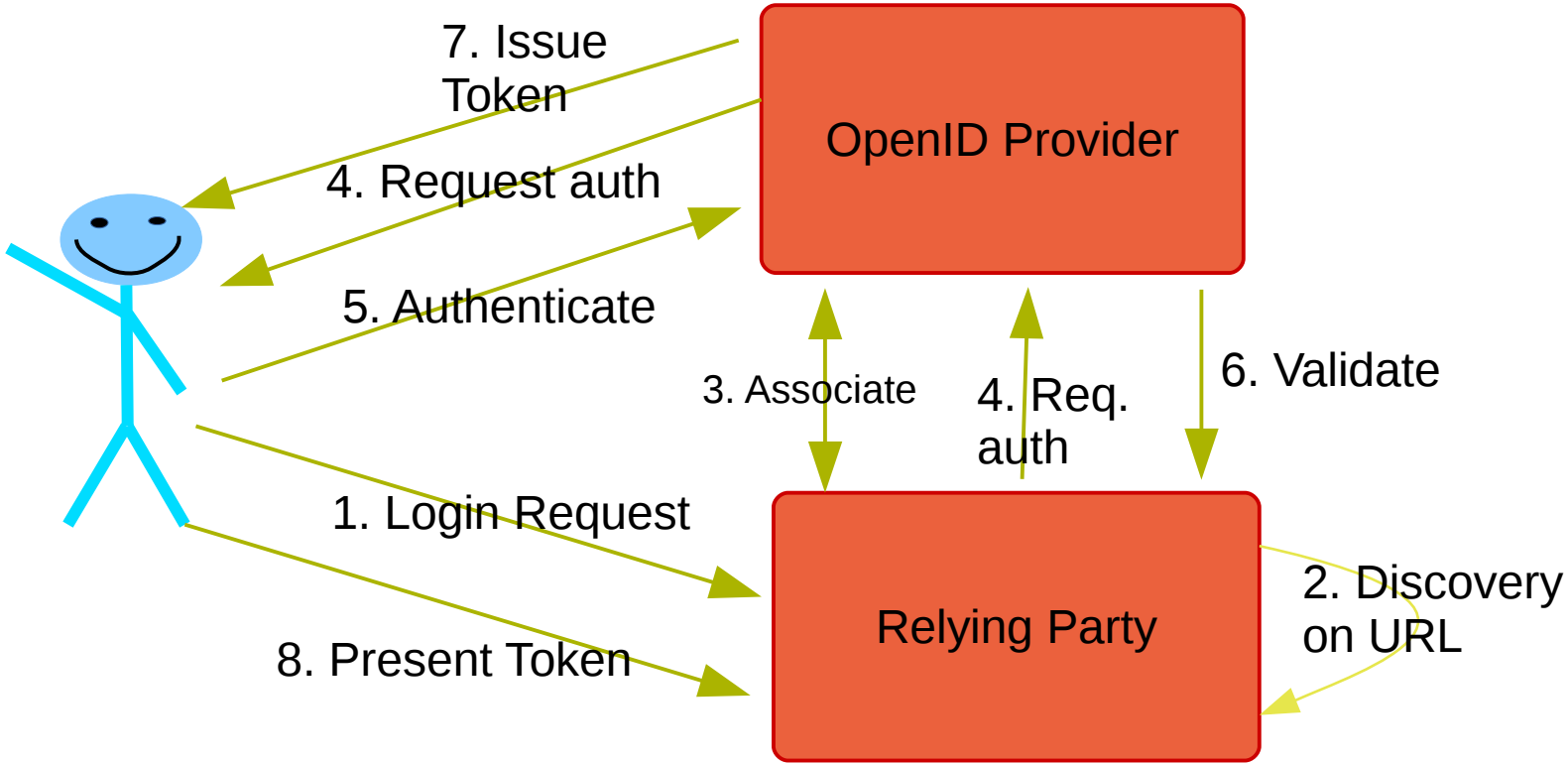
- Decentralized
- Identity is a URL
- You prove that you own that specific URL
- Like SAML, need to trust 3rd party to prove authentication
  - Or, if you want, you can run your own OpenID server

What is an OpenID Identity?

- Contains the location of the Identity Provider
- rcritten.id.fedoraproject.org

```
    <meta name="generator" content="Ipsilon">
        <link rel="openid2.delegate" href="http://rcritten.id.fedoraproject.org/">
        <link rel="openid.local_id" href="http://rcritten.id.fedoraproject.org/">
        <link rel="openid2.provider" href="https://id.fedoraproject.org/openid/">
        <link rel="openid.server" href="https://id.fedoraproject.org/openid/">
</head>
```

How does OpenID work?



OpenID Extensions

- Simple Registration Extension
- Attribute Exchange
- Teams

OpenID Use Cases

- Typically decentralized / user-centric
- Single Sign On
- Use single identity on multiple blogs, forums, e-mail, bug trackers

OpenID Providers

- FedOAuth
- Wordpress-OpenID
- Ipsilon
- MyOpenID (proprietary)

OpenID Relying Parties

- Wordpress-OpenID
- Flask-OpenID
- mod_auth_openid
- Bindings for most languages: Perl, .NET, python

Questions?

rcritten@redhat.com