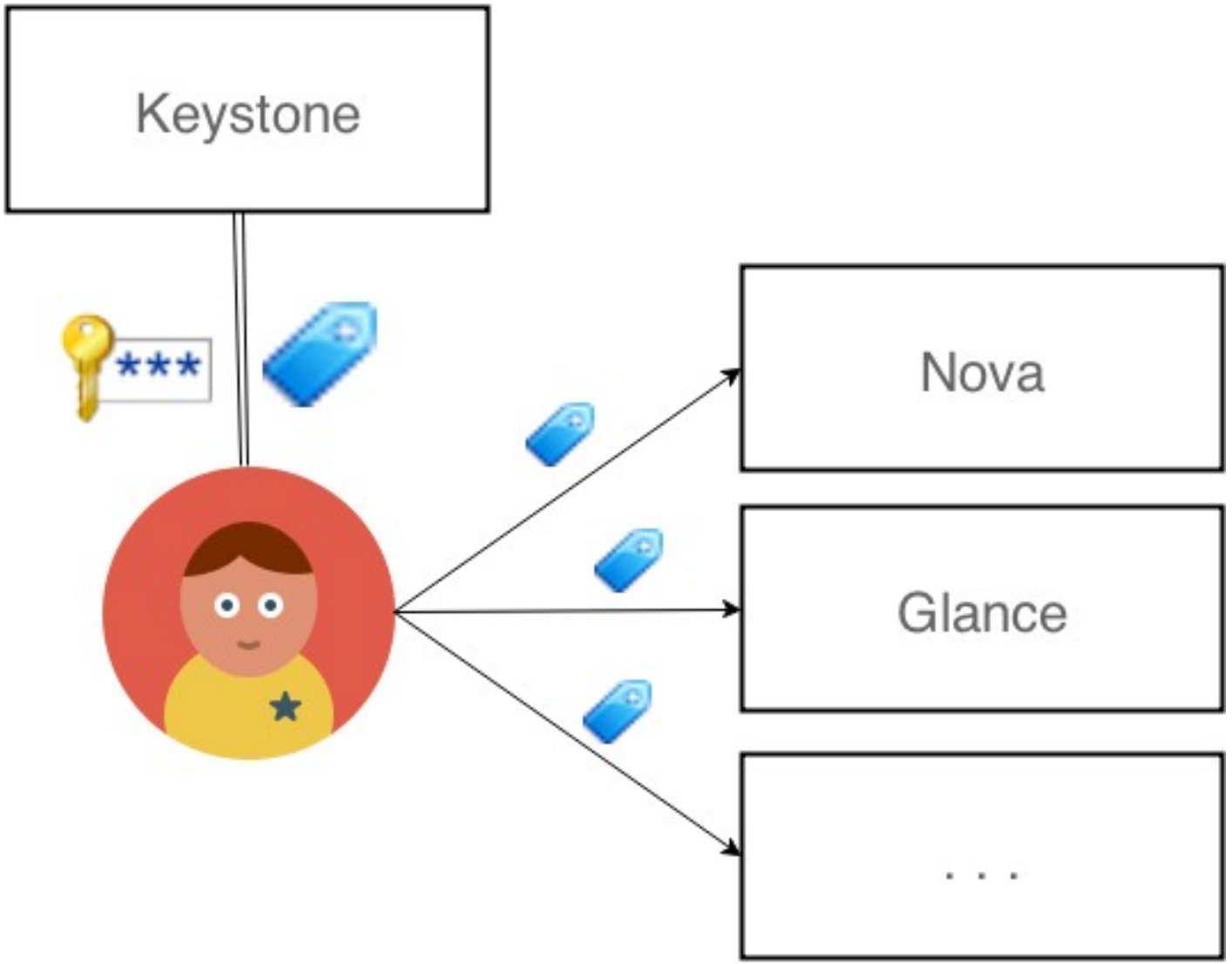
Keystone: Federated

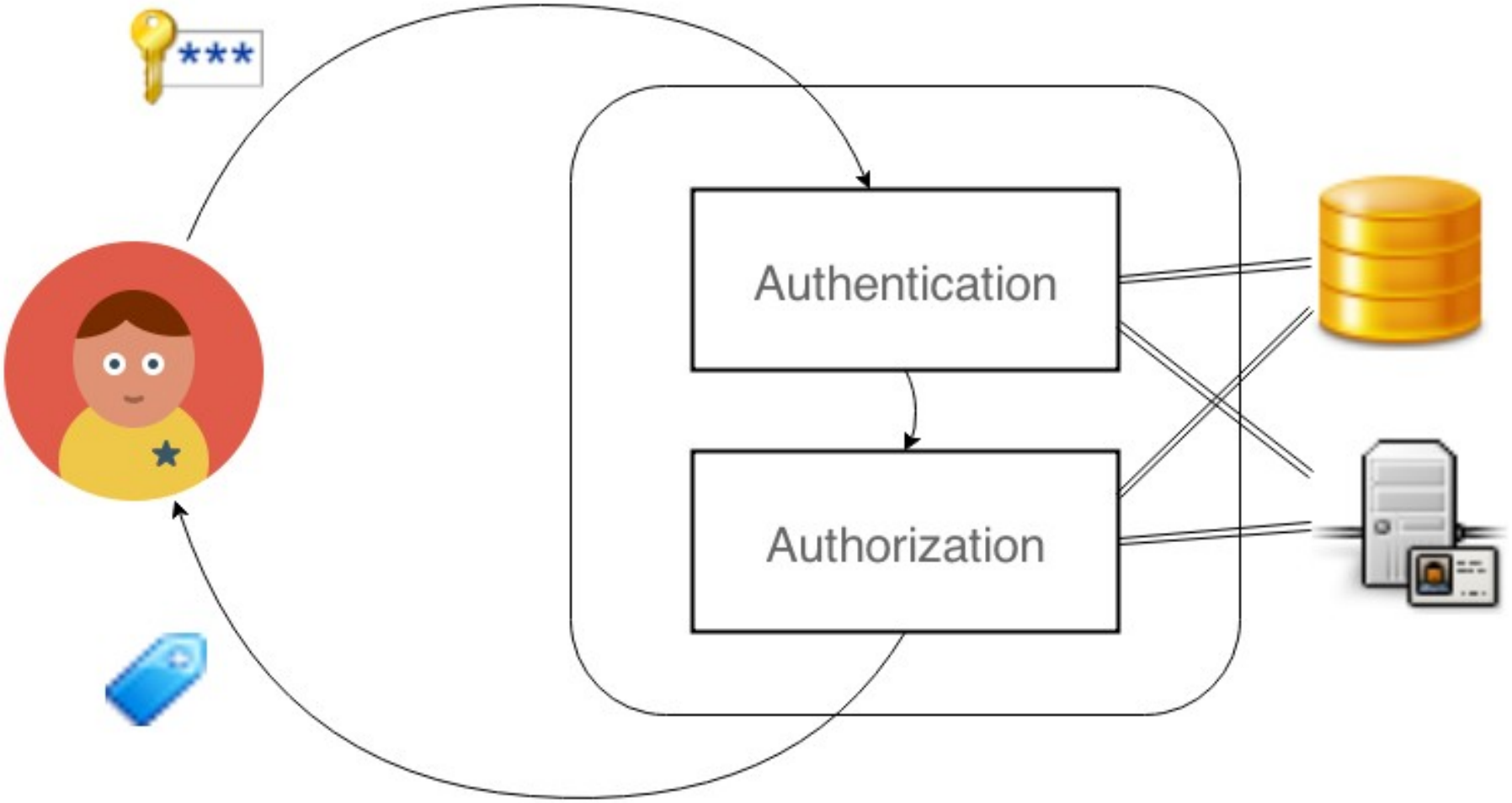
Jamie Lennox
1st Aug 2014

The OpenStack Identity Service

Token Flow



Token Issuing

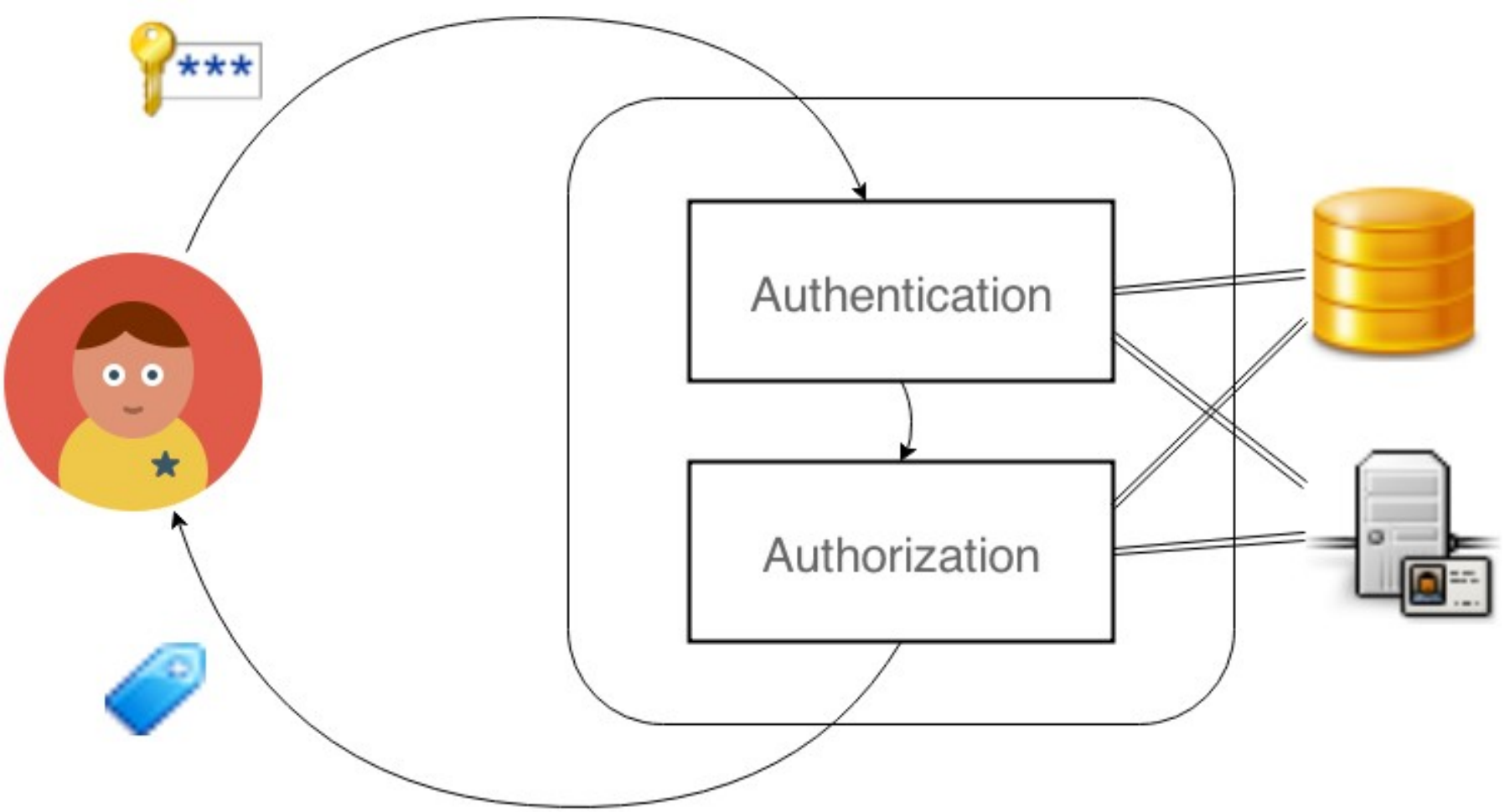


Federation

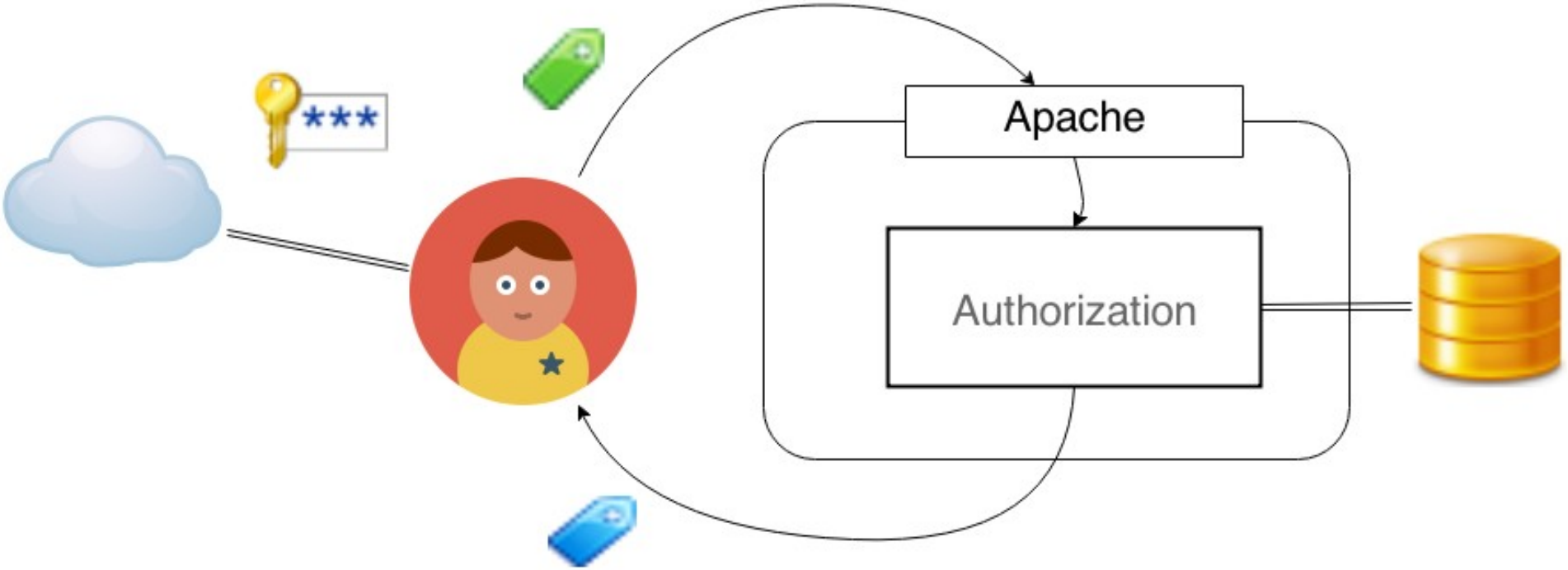
Why?

- Convenience
- Integration
  - Enterprise
  - Partnerships
- Migration and Interoperability
  - Multiple Clouds, Single Identity
- Security
  - One less identity provider

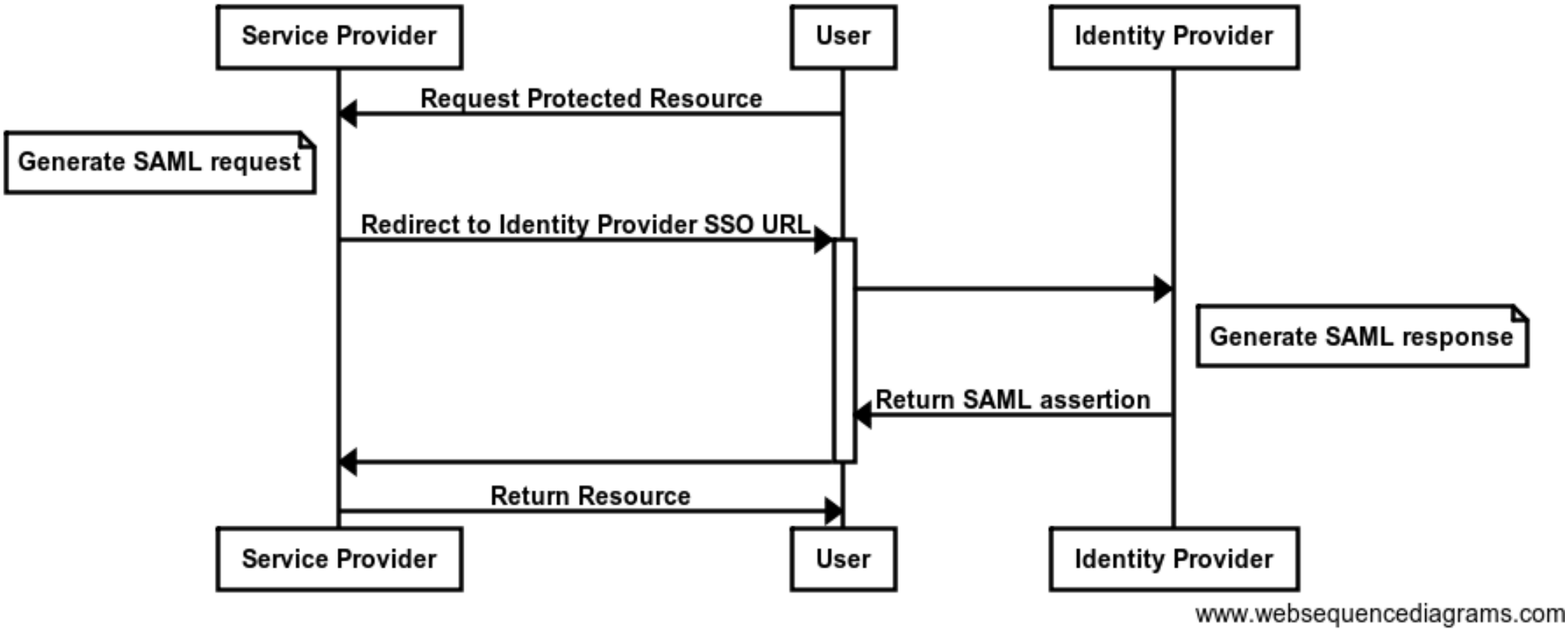
Identity Provider (IdPs)



Service Provider (SPs)



SAML


Service Provider
User
Identity Provider
Request Protected Resource
Generate SAML request
Redirect to Identity Provider SSO URL
Generate SAML response
Return SAML assertion
Return Resource
Service Provider
User
Identity Provider
www.websequencediagrams.com

```
<saml:AttributeStatement>
  <saml:Attribute Name="role">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xsi:type="xs:string"
                  >user</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="role">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xsi:type="xs:string"
                  >staff</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
<saml:AttributeStatement>
    <saml:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
                FriendlyName="sn"
                Name="urn:oid:2.5.4.4"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                x500:Encoding="LDAP"
                >
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xsi:type="xs:string"
                  >Lennox</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Environment Variables

MELLON_NAME_ID=_f4daafb1565ab2d75fdeab57b4717501b0cac62859
MELLON_NAME_ID_0=_f4daafb1565ab2d75fdeab57b4717501b0cac62859
MELLON_uid=jlennox
MELLON_uid_0=jlennox
MELLON_givenName=Jamie
MELLON_givenName_0=Jamie
MELLON_sn=**Lennox**
MELLON_sn_0=Lennox
MELLON_cn=Jamie Lennox
MELLON_cn_0=Jamie Lennox
MELLON_mail=jlennox@redhat.com
MELLON_mail_0=jlennox@redhat.com
MELLON_eduPersonPrincipalName=jlennox@rnd.feide.no
MELLON_eduPersonPrincipalName_0=jlennox@rnd.feide.no
MELLON_urn:oid:0_9_2342_19200300_100_1_1=jlennox
MELLON_urn:oid:0_9_2342_19200300_100_1_1_0=jlennox
MELLON_urn:oid:2_5_4_42=Jamie

Mapping

- Convert IdP Assertions to OpenStack Roles
  - Different roles mean different things on different IdPs
- Mapping:
  - The presence/value of which remote attributes,
  - Lead to what user data on the local server.
- Users don't exist in Keystone
  - Groups can have roles

Mapping Snippet

```
"rules": [
    {
        "local": [
            {
                "user": {
                    "name": "{0} {1}",
                    "id": "{2}"
                }
            },
            {
                "group": {
                    "id": "37ebd1d9e3...
                }
            }
        ],
```

```
        "remote": [
            {
                "type": "givenName"
            },
            {
                "type": "sn",
                "any_one_of": ["Lennox"]
            },
            {
                "type": "uid"
            },
            {
                "type": "role",
                "any_one_of": ["staff"]
            }
        ]
    }
]
```

Identity Provider CRUD

- Configuring Identity Providers.
  - /v3/OS-FEDERATION/identity_providers/{idp_id}
- Configure a Mapping.
  - /v3/OS-FEDERATION/mappings/{mapping_id}
- Protocols are managed per Identity Provider
  - Allows an Identity Provider to use multiple protocols
  - A protocol contains a mapping.
  - /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol}
- Tokens are issued via the protocol
  - /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol}/auth

Today

- **It works**, but…
  - SAML2 ECP
  - Client side is in review
- Framework and the Mapper.

Future

- Anything you can map...
  - mod_auth_openid
  - mod_identity_lookup
  - AbFab
- You could even...
  - mod_auth_kerb
  - mod_auth_digest
- **Keystone**

Credits

University of Kent

Thanks

Questions

jamielennox on freenode

jamielennox@redhat.com

@jamielennox_

Image Credits

- Keystone: http://buffaloah.com/a/DCTNRY/k/keystone_fairfax.JPG
- Federation: http://pixabay.com/en/networks-internet-facebook-social-232313/
- SAML: http://www.websequencediagrams.com/?lz=cGFydGljaXBhbnQgU2VydmljZSBQcm92aWRlcgoAEQxVcwACD0lkZW50aXR5ACUKClVzZXItPgA3EDogUmVxdWVzdCBQcm90ZWN0ZWQgUmVzb3VyY2UKbm90ZSBsZWZ0IG9mAHAROiBHZW5lcmF0ZSBTQU1MIHIAQgYKAIEZEC0-K1VzAGMGZGlyZWN0IHRvAIEOEiBTU08gVVJMAIEgBwCBLxE6IACBCAZyaWdoAIEKBQAPEwCBABBzcG9uc2UKAIF7ES0-AIEMBVJldHVybgCBNwZhc3NlcnRpb24AgiAHLQCCFxEAgUUTAIFPCABCBQCCLQg&s=patent
- Diagrams: https://draw.io