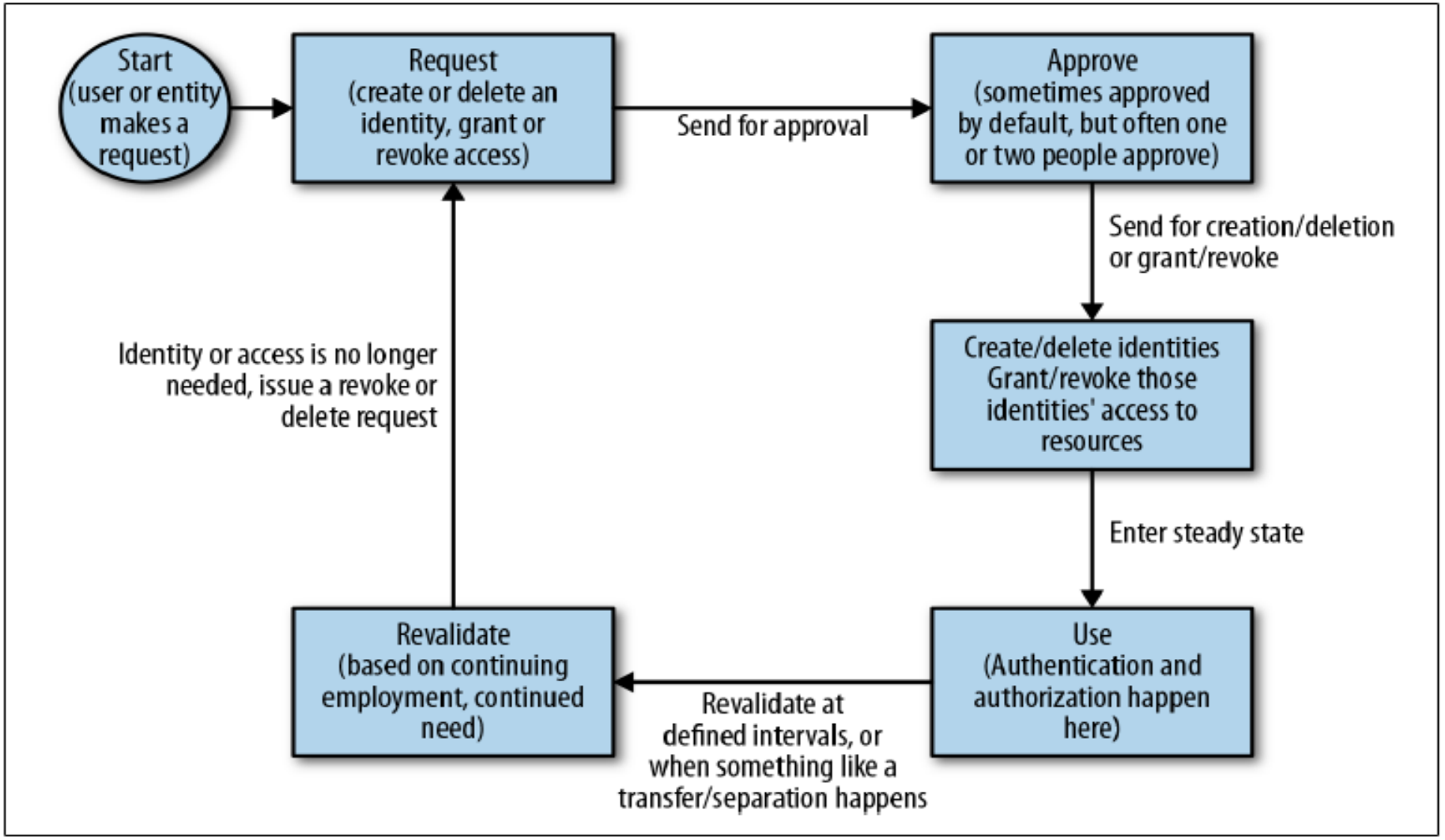
# IAM in Cloud Computing

Dr. Amit Praseed

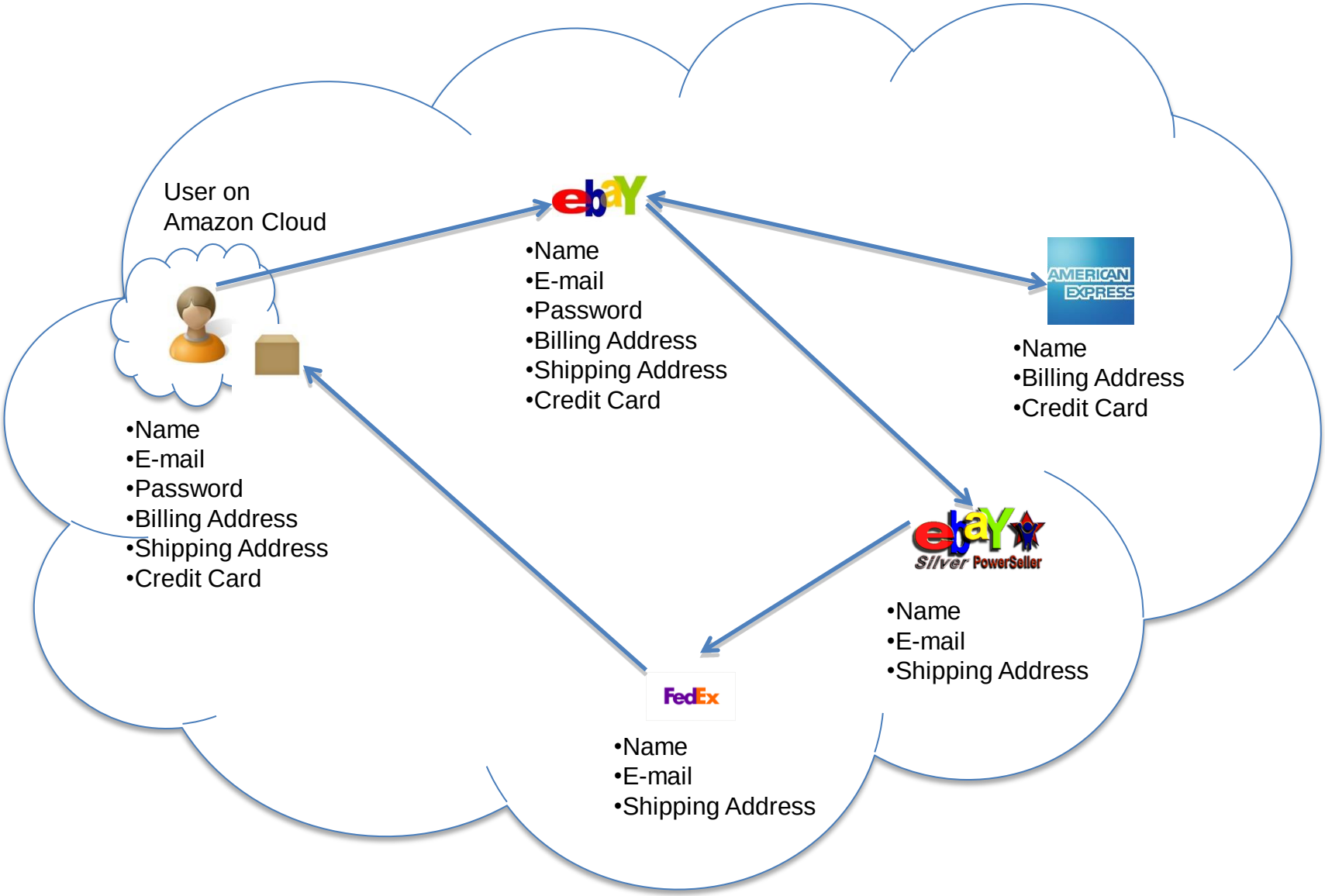
# Identity and Access Management

- Each entity (such as a user, administrator, or system) needs an identity
  - The process of verifying that identity is called *authentication*
- Access management is about ensuring that entities can perform only the tasks they need to perform.
  - The process of checking what access an entity should have is called *authorization*

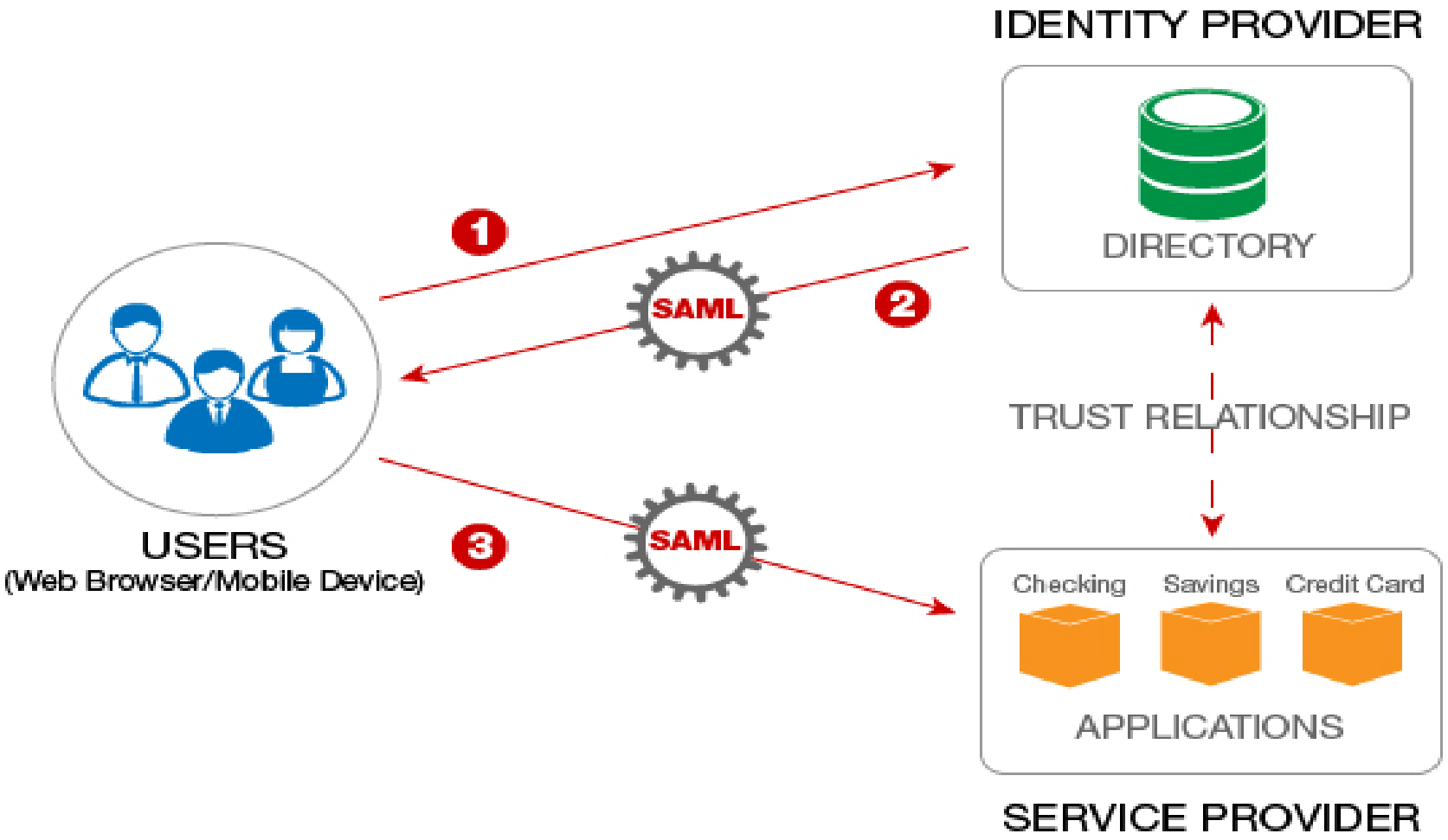
# IAM Life Cycle



# So many Identities!!!



# SSO to the Rescue!



# Protocols for SSO

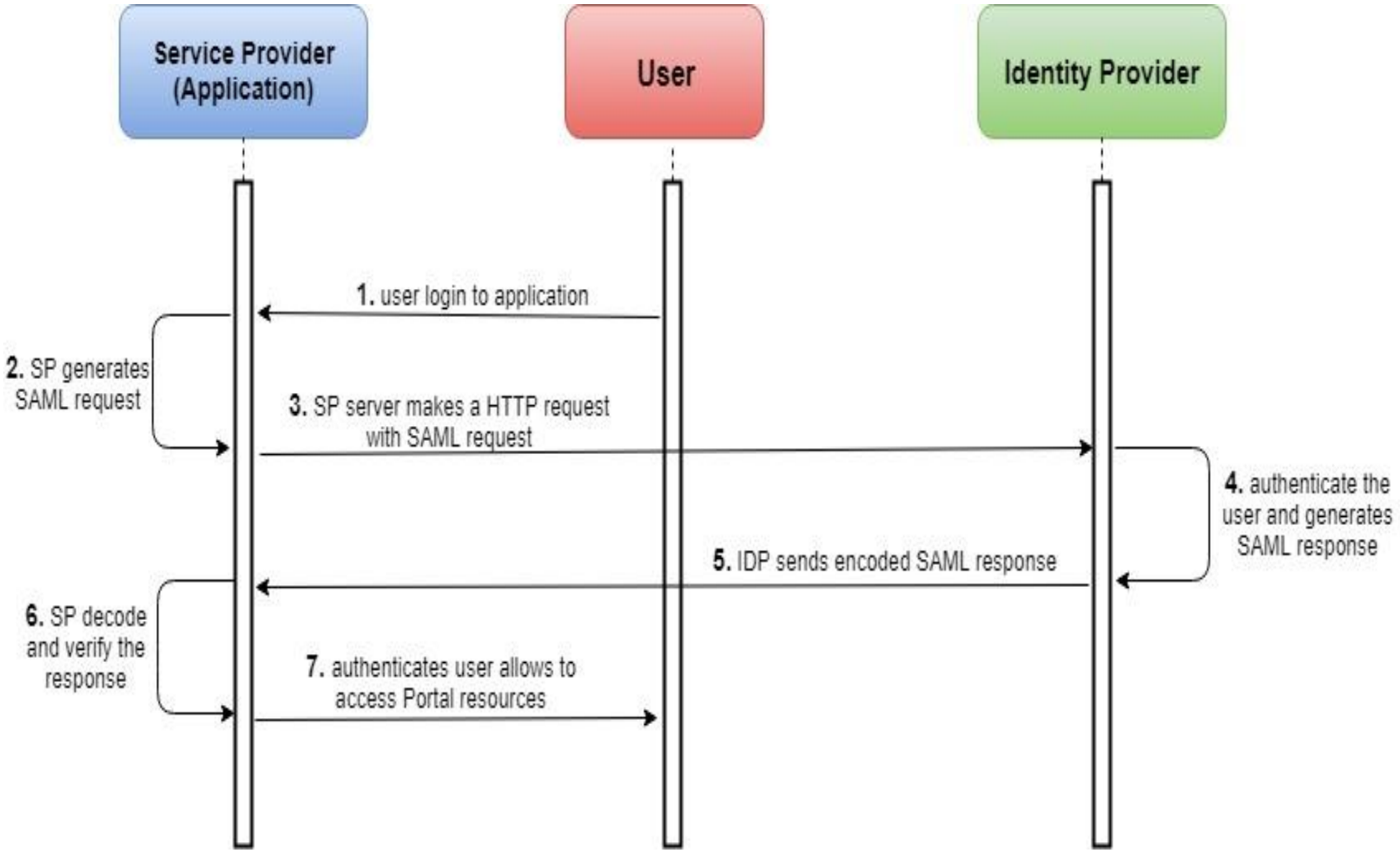
- There are three popular mechanisms that are used to provide SSO
  - Security Assertion Markup Language (SAML)
  - Open Authorization (OAuth)
  - OpenID

# SAML

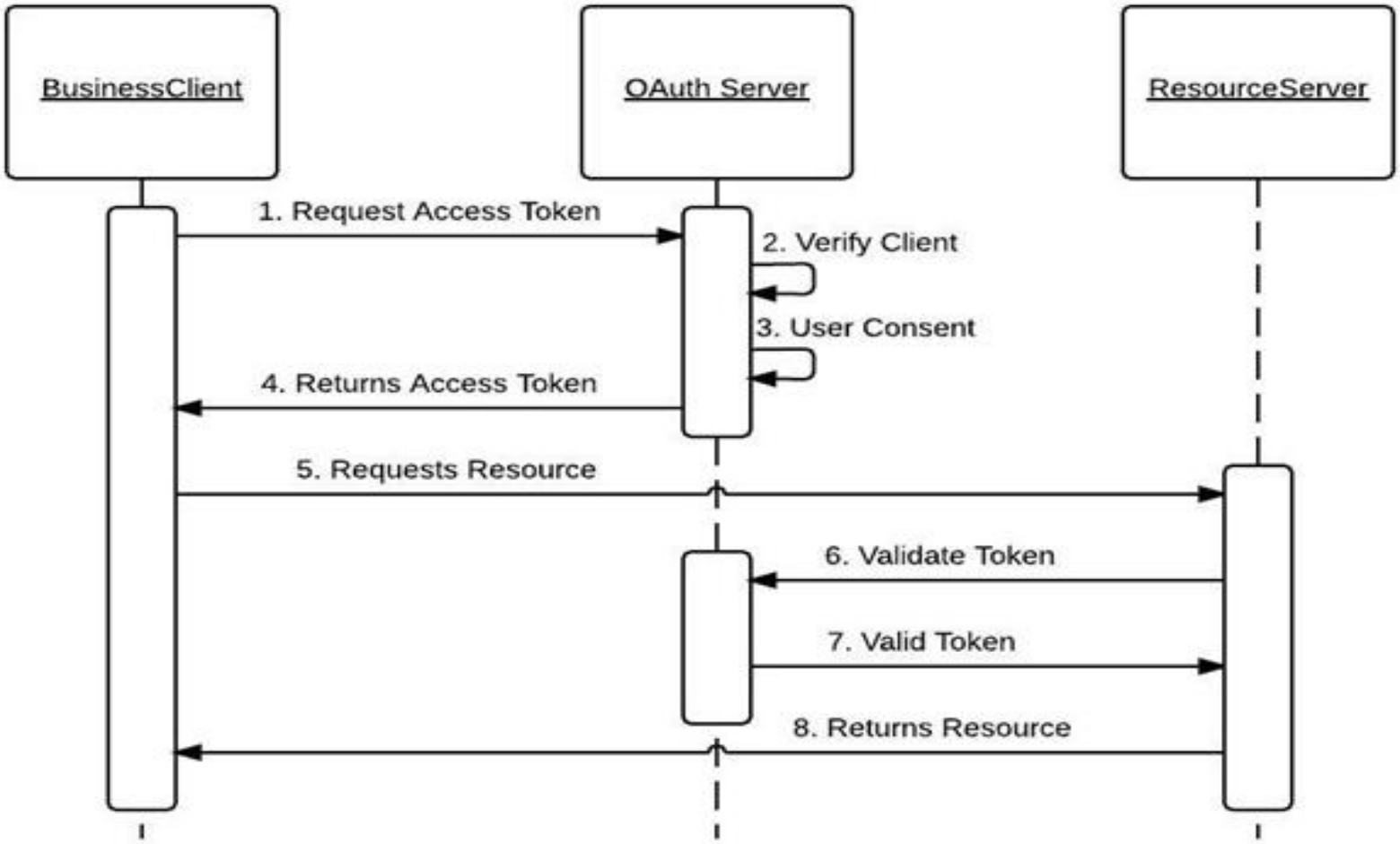
- SAML was developed in the early 2000s
  - define an XML framework for exchanging authentication and authorization information
  - allows a user's identity to be passed from one place to another with digitally signed XML (eXtensible Markup Language) documents.
  - SAML Info: Version, ID, ProviderName, IssueInstant, Destination, ProtocolBinding, AssertionConsumerServiceURL, and Issuer

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="ONELOGIN_809707f0030a5d00620c9d9df97f627afe9dcc24"
Version="2.0" ProviderName="SP test" IssueInstant="2014-07-16T23:52:45Z"
Destination="http://idp.example.com/SSOService.php" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="http://sp.example.com/demo1/index.php?acs">
    <saml:Issuer>http://sp.example.com/demo1/metadata.php</saml:Issuer>
    <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
    AllowCreate="true" />
    <samlp:RequestedAuthnContext Comparison="exact">
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

# SAML Workflow



# OAuth Workflow



# SSO and Privacy

- Cloud introduces several issues to IDM
  - Collusion between Cloud Services
    - Users have multiple accounts associated with multiple service providers.
    - Sharing sensitive identity information between services can lead to undesirable mapping of the identities to the user.
  - Lack of trust
    - Cloud hosts are untrusted
    - Use of Trusted Third Party is not an option
  - Loss of control
    - Service-centric IDM Model

# SSO and Privacy

- Anonymous Identification
  - Based on cryptographic zero knowledge proofs
- Multi party Authentication
  - Based on secure multi party computation
  - Information is distributed and managed by multiple identity providers, all of whom hold non-overlapping information
  - Unless *k* IdPs collude, user information cannot be effectively leaked