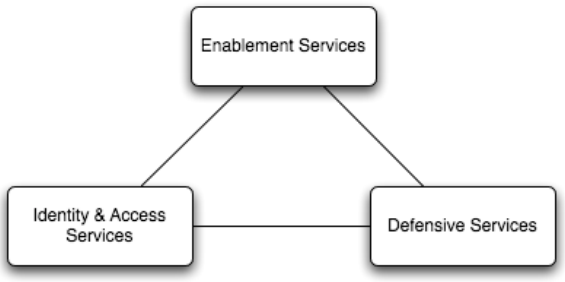
Identity & Access Management

Presentation by Gunnar Peterson
www.arctecgroup.net

ARCTEC

A more pragmatic goal

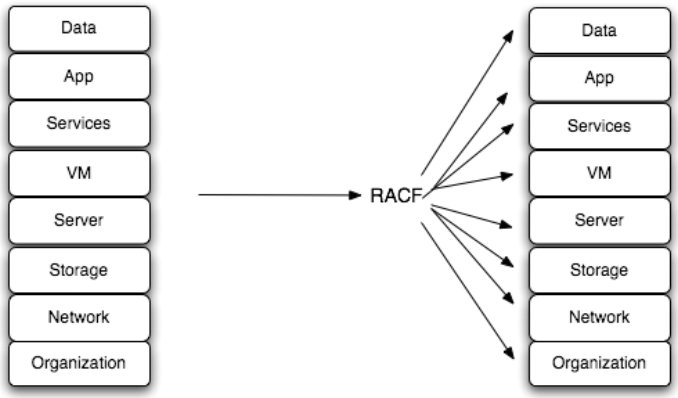


- **Identity & Access Services**: Letting good guys do their work - Claims enabled services
- **Defensive Services:** keeping bad guys out - conservative services that deal with threats and vulnerabilities
- **Enablement Services:** making it all work - services managing business enabling such as capabilities provisioning, federation, identity, and secure integration

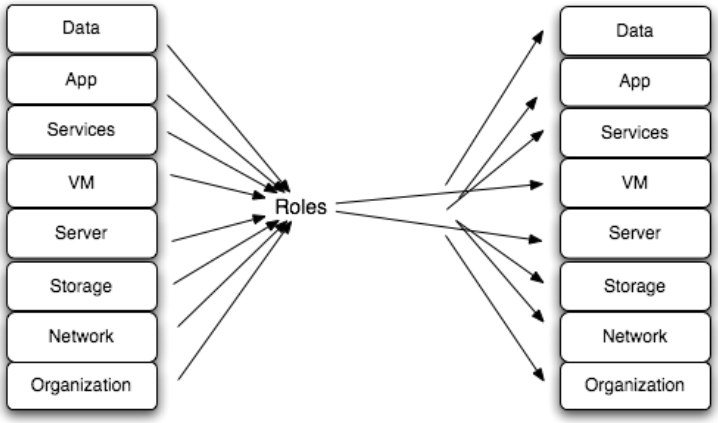
Brief History of Access Control

- Reference Monitor: defines access control properties
  - Always invoked
  - Tamper proof
  - Small enough to be analyzed
- RACF/Top Secret: resource-centric
- RBAC: role/session-centric
- ABAC/CBAC: tokens used to evaluate claims about subjects (attributes)
- PBAC: policies for consistent governance

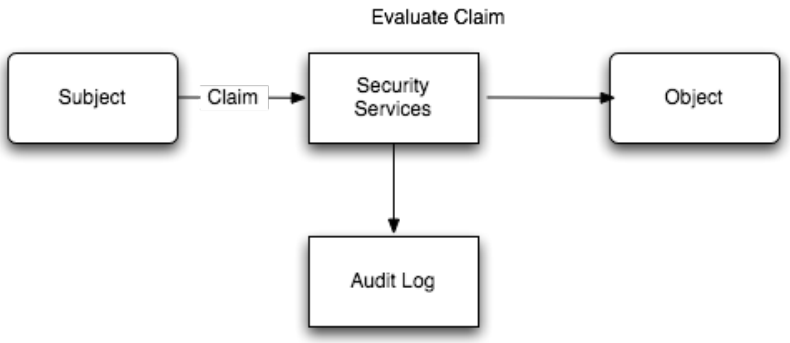
Resource Centric Access Control



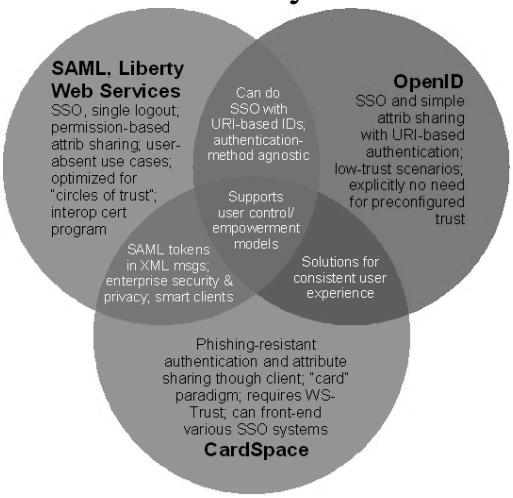
Role Based Access Control



CBAC: Claims Based Access Control

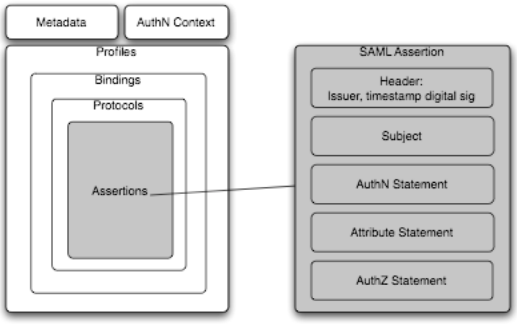


The Identity Venn



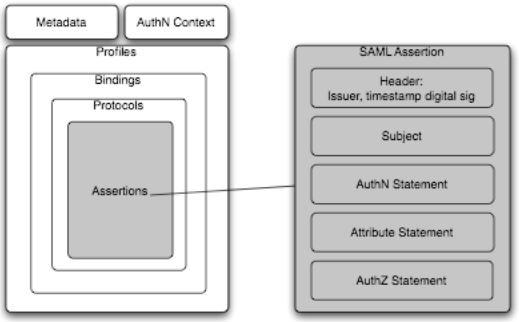
Source, Eve Maler http://www.xmlgrrl.com/blog

SAML Assertion



- Headers & Control Information
  - SAML Issuer
  - Timers
  - XML Encryption spec supports:
    - Block Encryption: TRIPLE DES, AES-128, AES-256
    - Key Transport: RSA-v1.5, RSA-OAEP
  - Digital Signature spec supports:
    - Digest: SHA1
    - MAC: HMAC-SHA1
    - XML Canonicalization: CanonicalXML (Without comments)
    - Transform: Enveloped Signature
    - Signature: RSAwithSHA1 (recommended in XML Signature but needed for interoperability)

SAML Assertion

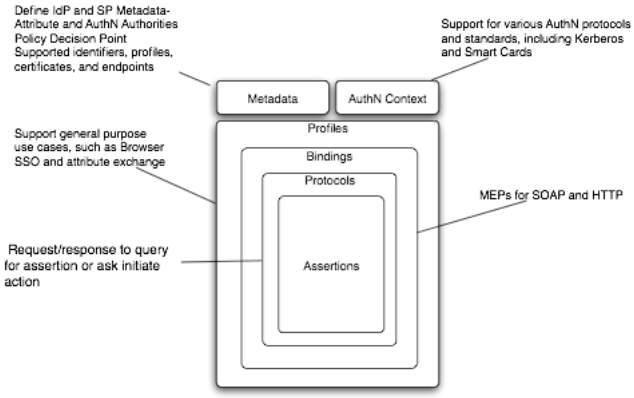


Authentication Statement
- How was the user authenticated

Attribute Statement
- Is there any additional identity information about the user

Authorization Decision Statement
- Have any authorization decisions been made for this user

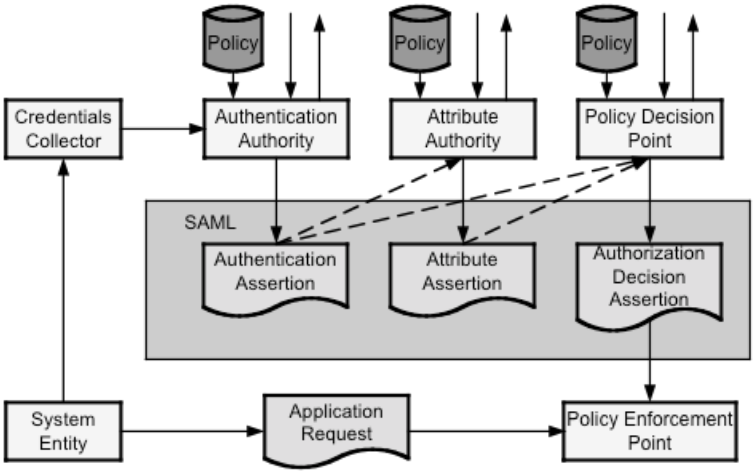
SAML 2.0



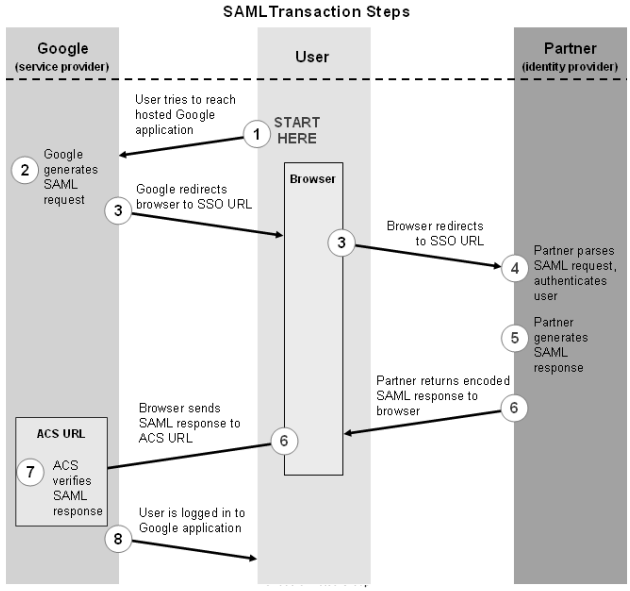
```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:
2.0:assertion"
   Version="2.0" IssueInstant="2005-04-01T16:58:33.173Z">
   <saml:Issuer>http://authority.example.com/</saml:Issuer>
<!-- signature by the issuer over the assertion -->
       <ds:Signature>...</ds:Signature>
       <saml:Subject>
       <saml:NameID format="urn:oasis:names:tc:SAML:2.0:nameid-
       format:persistent">
       jygH5F90l
       </saml:NameID>
   </saml:Subject>
       <saml:AuthnStatement
       AuthnInstant="2005-04- 01T16:57:30.000Z"
       SessionIndex="6345789">
       <saml:AuthnContext>
         <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspor
       </saml:AuthnContextClassRef>
       </saml:AuthnContext>
       </saml:AuthnStatement>
</saml:Assertion>
```

Source Paul Madsen http://www.xml.com/pub/a/2005/01/12/saml2.html

SAML Producer Consumer Model



- Source http://lists.oasis-open.org/archives/security-services/200506/msg00031.html



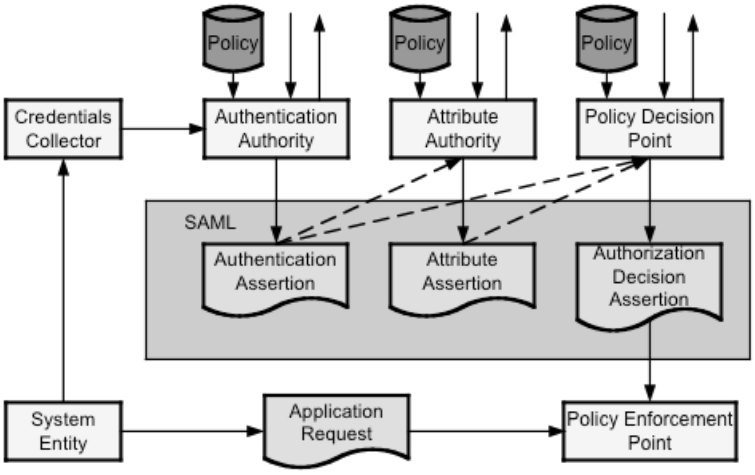
SAML Request

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   ID="[[AUTHN_ID]]"
   Version="2.0"
   IssueInstant="[[ISSUE_INSTANT]]"
   ProtocolBinding="urn:oasis:names.tc:SAML:2.0:bindings:HTTP-Redirect"
   ProviderName="[[PROVIDER_NAME]]"
   AssertionConsumerServiceURL="[[ACS_URL]]"/>
```

SAML Response

```
<samlp:Response ID="[[RESPONSE_ID]]" IssueInstant="[[ISSUE_INSTANT]]" Version="2.0"
   xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </samlp:Status>
   <Assertion ID="[[ASSERTION_ID]]"
      IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
      xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
      <Issuer>https://www.opensaml.org/IDP</Issuer>
      <Subject>
         <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress">
            [[USERNAME_STRING]]
         </NameID>
         <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
      </Subject>
      <Conditions NotBefore="[[NOT_BEFORE]]"
         NotOnOrAfter="[[NOT_ON_OR_AFTER]]">
      </Conditions>
      <AuthnStatement AuthnInstant="[[AUTHN_INSTANT]]">
…
```


SAML Producer Consumer Model



- Source http://lists.oasis-open.org/archives/security-services/200506/msg00031.html

```
 <saml:Assertion
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
   Version="2.0"
   IssueInstant="2004-12-05T09:22:05Z">
   <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
   <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</
ds:Signature>
   <saml:Subject>
     <saml:NameID
       Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">
       3f7b3dcf-1674-4ecd-92c8-1544f346baf8
     </saml:NameID>
     <saml:SubjectConfirmation
       Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
       <saml:SubjectConfirmationData
         InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
         Recipient="https://sp.example.com/SAML2/SSO/POST"
         NotOnOrAfter="2004-12-05T09:27:05Z"/>
     </saml:SubjectConfirmation>
   </saml:Subject>
```



```
<saml:Conditions
    NotBefore="2004-12-05T09:17:05Z"
    NotOnOrAfter="2004-12-05T09:27:05Z">
    <saml:AudienceRestriction>
      <saml:Audience>https://sp.example.com/SAML2</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement
    AuthnInstant="2004-12-05T09:22:00Z"
    SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
       </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute
      xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
      FriendlyName="eduPersonAffiliation">
      <saml:AttributeValue
        xsi:type="xs:string">member</saml:AttributeValue>
      <saml:AttributeValue
        xsi:type="xs:string">staff</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

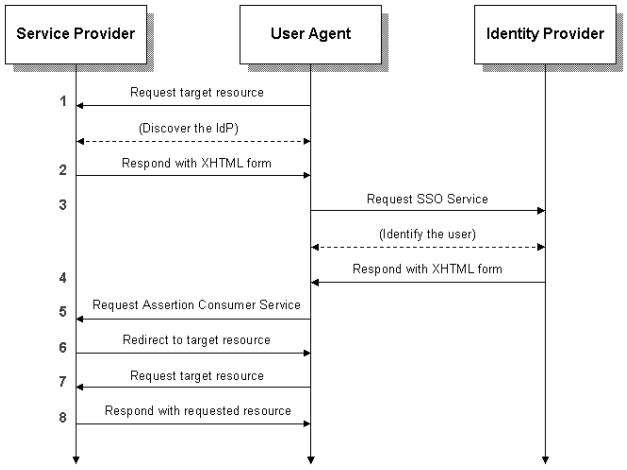
```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="aaf23196-1773-2113-474a-fe114412ab72"
  Version="2.0"
  IssueInstant="2004-12-05T09:21:59Z"
  AssertionConsumerServiceIndex="0"
  AttributeConsumingServiceIndex="0">
  <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
  <samlp:NameIDPolicy
    AllowCreate="true"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
</samlp:AuthnRequest>
```

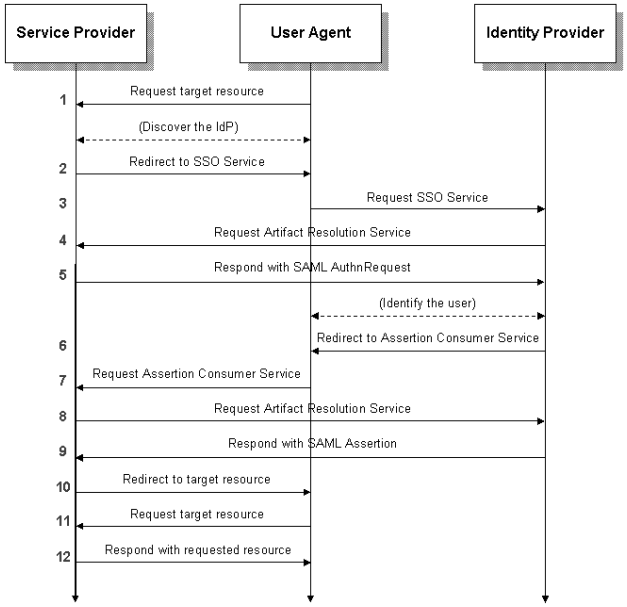


```
<samlp:ArtifactResolve
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_cce4ee769ed970b501d680f697989d14"
  Version="2.0"
  IssueInstant="2004-12-05T09:21:58Z"
  Destination="https://sp.example.com/SAML2/ArtifactResolution">
  <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
  <ds:Signature
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  <samlp:Artifact>AAQAAMh48/1oXIM
+sDo7Dh2qMp1HM4IF5DaRNmDj6RdUmllwn9jJHyEgIi8=</samlp:Artifact>
</samlp:ArtifactResolve>
```

```
https://idp.example.org/SAML2/SSO/Artifact?SAMLart=artifact
```

```
<samlp:ArtifactResponse
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="_d84a49e5958803dedcff4c984c2b0d95"
  InResponseTo="_cce4ee769ed970b501d680f697989d14"
  Version="2.0"
  IssueInstant="2004-12-05T09:21:59Z">
  <ds:Signature
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_306f8ec5b618f361c70b6ffb1480eade"
    Version="2.0"
    IssueInstant="2004-12-05T09:21:59Z"
    Destination="https://idp.example.org/SAML2/SSO/Artifact"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
    AssertionConsumerServiceURL="https://sp.example.com/SAML2/SSO/Artifact">
    <saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
    <samlp:NameIDPolicy
      AllowCreate="false"
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>
  </samlp:AuthnRequest>
</samlp:ArtifactResponse>
```



Where does SAML fit?

Threat	Security Service	Data	Method	Channel
Spoofing	Authentication	SAML	SAML	
Tampering	Digital Signature	SAML		
Dispute	Audit Logging			
Information Disclosure	Encryption	SAML		
Denial of Service	Availability			
Elevation of privilege	Authorization, Input validation	SAML		

Decentralized Policy

– Using XACML for consistent policy management and enforcement

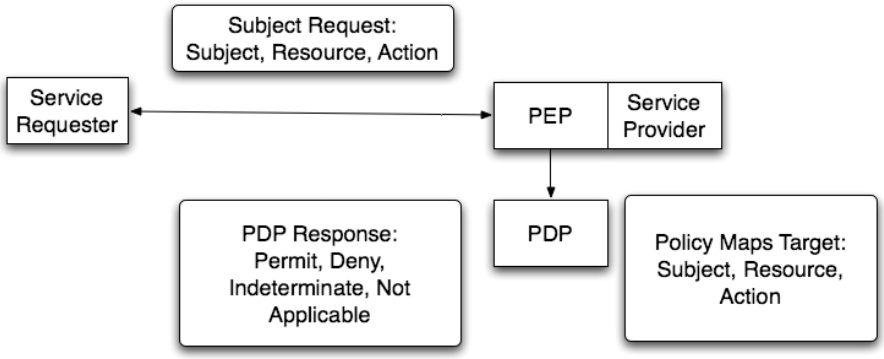
XACML

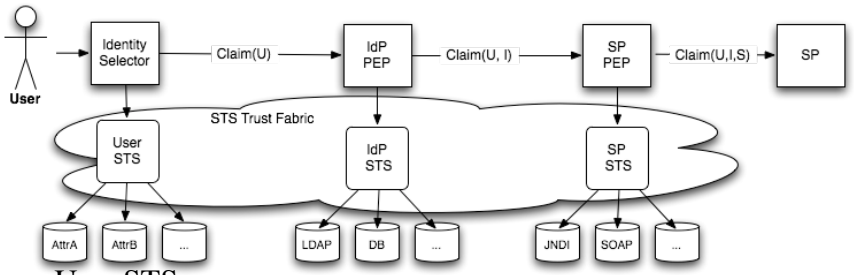
- Goal: Consistent access control policy and enforcement across technical and organizational domains
- Interoperates with SAML 2.0
  - SAML Attributes
  - SAML Authorization decisions
  - XACML's policy language describes how SP should handle SAML
- Policy languages are immature

XACML Concepts

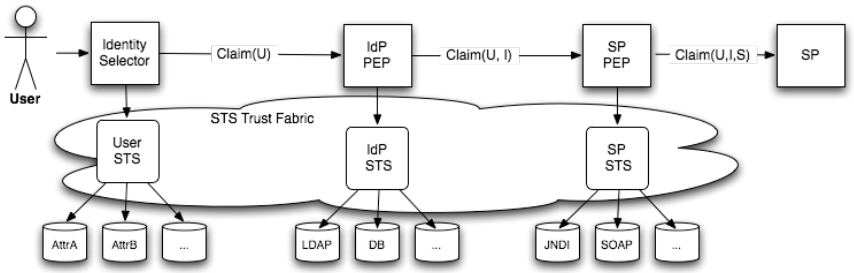
- Policy/ Policysets
  - Targets - a set of conditions for subjects, resources and actions to fulfill. Allows for granular definition and enforcement, e.g. at a service's method level
  - Rules - conditions, effects, and targets that are evaluated to grant access
  - Policy Enforcement Point: assembles the requester's attributes and sends to PDP
  - Policy Decision Point: evaluates and responds to request
  - Attributes: set of verifiable attributes, may be SAML attributes

XACML Overview

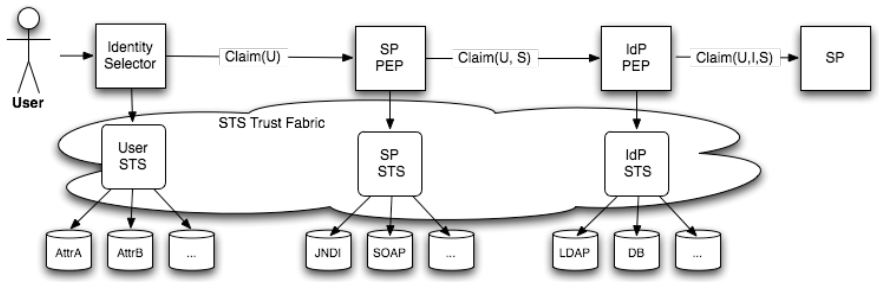




- User STS
  - Responsibilities:
    - Map user to set of verifiable claims
    - Select identity to authenticate
    - Select identity and/or attribute claims to release
    - Enable usability of security protocols
    - Optionally enable multi-factor authN
    - Optionally, provider anonymizers and pseudonymizers
  - Collaborations: The user STS collaborates with
    - Identity Provider for authentication
    - Attribute stores
    - Required security protocols – 2 factor, etc.
    - Work in user environment with usability-centric tooling – e.g. Azigo, Cardspace, browser plugins, et al.



- IdP STS
  - Responsibilities:
    - Subject ←> claim mapping
    - Map requests and responses to token(s) based on policy
    - Route and transform requests and responses based on policy
    - Policy based payload access
  - Collaborations:
    - User stores
    - Directories
    - Multi-factor



- SP STS
  - Responsibilities:
    - Object/resource <-> claim mapping
    - Mapping requests and responses to token(s) based on policy
    - Route and transform requests and responses based on policy
    - Policy based payload access
  - Collaborations:
    - Objects under management, e.g. JNDI trees, JDBC connections, databases, Web Service methods, et. Al.