SAML basics

A technical introduction to the Security Assertion Markup Language

WWW2002

Eve Maler, XML Standards Architect
XML Technology Center
Sun Microsystems, Inc.

Agenda

- The problem space
- SAML concepts
- Walking through scenarios
- Status of SAML and helpful resources
- Your questions

Agenda

- The problem space
  - Why invent SAML at all?
  - What are the use cases that drive SAML’s design?
- SAML concepts
- Walking through scenarios
- Status of SAML and helpful resources

Is there even a problem to solve?

- Standards are emerging for many facets of collaborative e-commerce
  - Business transactions (e.g., ebXML)
  - Software interactions (e.g., SOAP)
- And some sophisticated access management solutions do exist
  - For example, dozens of companies provide "single sign-on" (SSO) solutions
- But…

Where do the problems lie?

- …but communicating the security properties of these interactions isn’t well standardized
- And the solutions don’t interoperate at all
- And thus there’s lower deployment of interesting access management solutions, especially on the web
    - Like single sign-on (SSO)
- Web-based commerce shows the need for federation and standardization
    - For cost-effectiveness
    - For interoperability among solutions
    - For a more cohesive user experience

Use cases for sharing security information

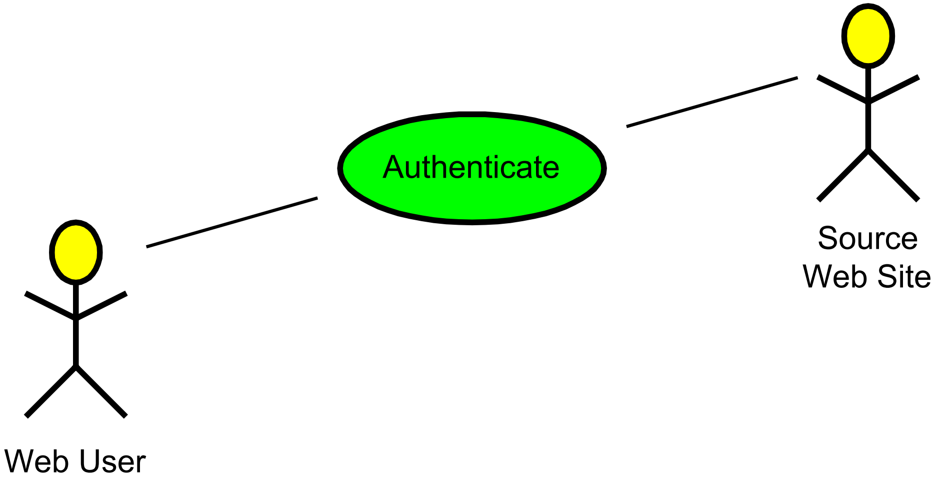
- SAML developed three “use cases” to drive its requirements and design:
  1. Single sign-on (SSO)
  2. Distributed transaction
  3. Authorization service
- Each use case has one or more “scenarios” that provide a more detailed roadmap of interaction

#1: Single sign-on (SSO)

- Logged-in users of analyst research site SmithCo are allowed access to research produced by sister site JonesCo, where the two sites might be in a “federation”

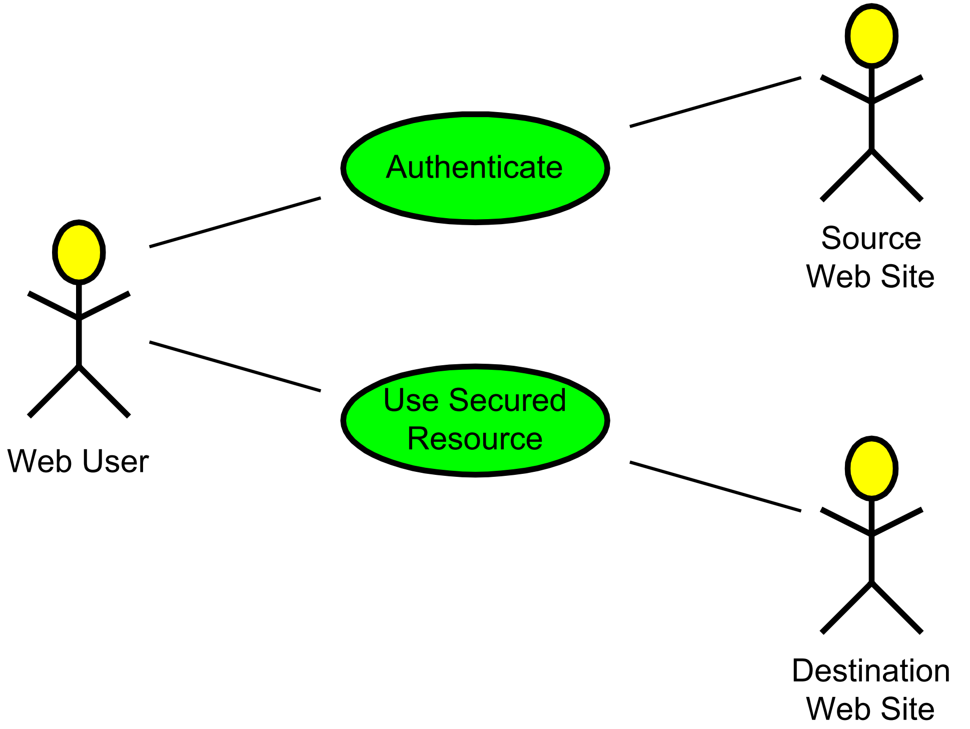
#1: Single sign-on (SSO)

- Logged-in users of analyst research site SmithCo are allowed access to research produced by sister site JonesCo, where the two sites might be in a "federation"



#1: Single sign-on (SSO)

- Logged-in users of analyst research site SmithCo are allowed access to research produced by sister site JonesCo, where the two sites might be in a “federation”

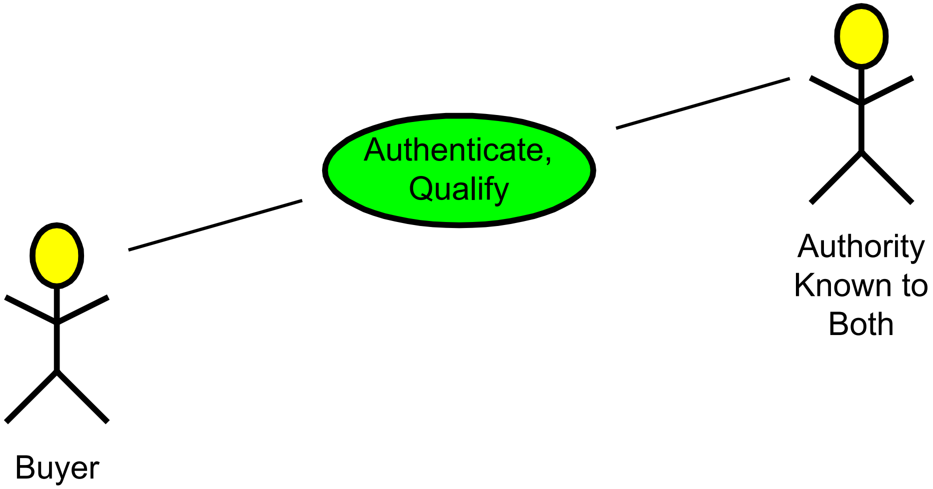


#2: Distributed transaction

- Employees at SmithCo are allowed to order office supplies from OfficeBarn if they are authorized to spend enough

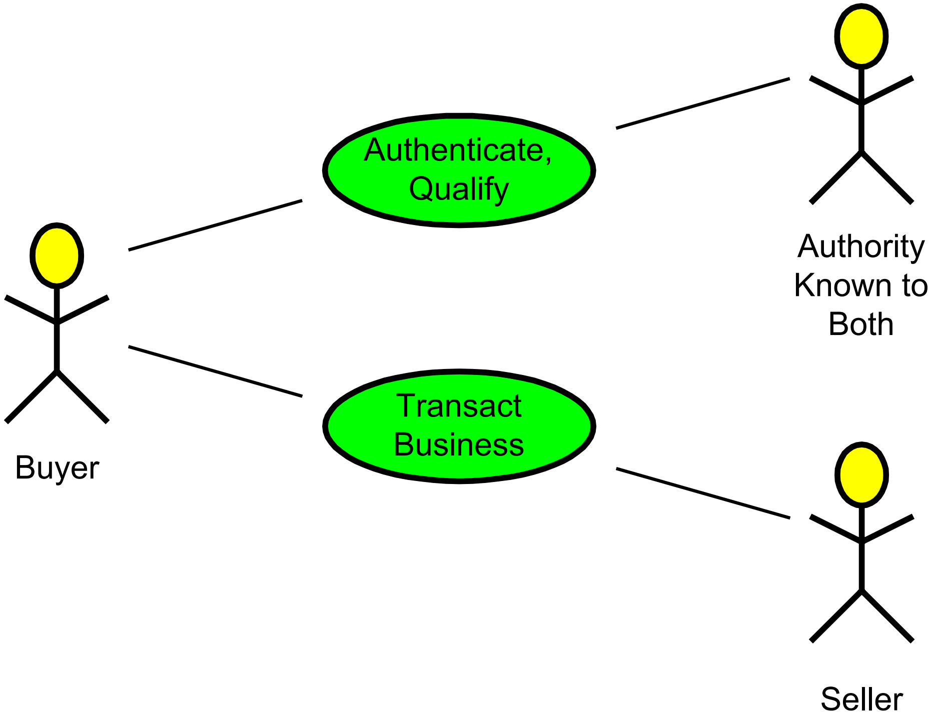
#2: Distributed transaction

- Employees at SmithCo are allowed to order office supplies from OfficeBarn if they are authorized to spend enough



#2: Distributed transaction

- Employees at SmithCo are allowed to order office supplies from OfficeBarn if they are authorized to spend enough

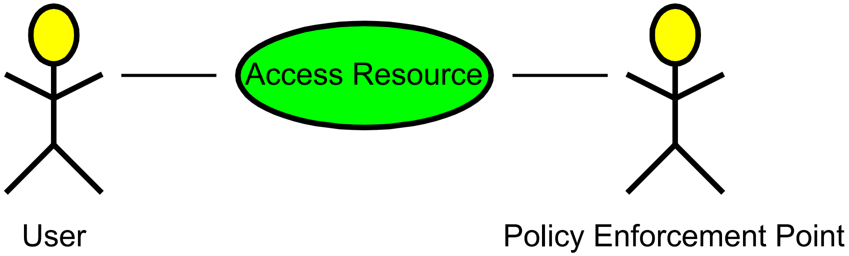


#3: Authorization service

- Employees at SmithCo order office supplies directly from OfficeBarn, which performs its own authorization

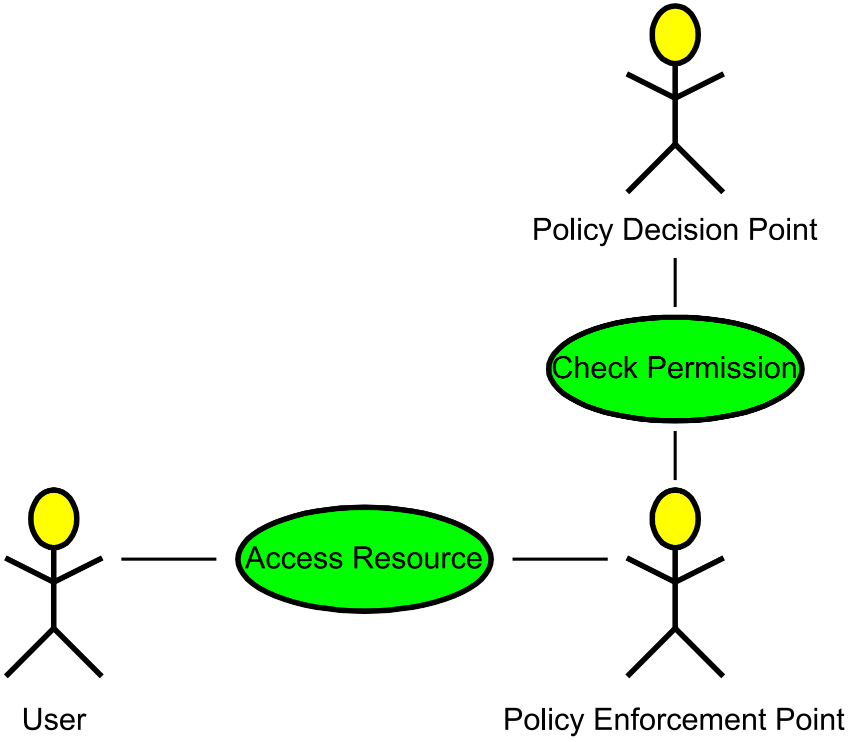
#3: Authorization service

- Employees at SmithCo order office supplies directly from OfficeBarn, which performs its own authorization



#3: Authorization service

- Employees at SmithCo order office supplies directly from OfficeBarn, which performs its own authorization



What’s needed to accomplish all this

- A standard XML message format
  - It’s just data traveling on any wire
  - No particular API mandated
  - Lots of XML tools available
- A standard message exchange protocol
  - Clarity in orchestrating how you ask for and get the information you need
- Rules for how the messages ride “on” transport protocols and “in” application contexts
  - For better interoperability

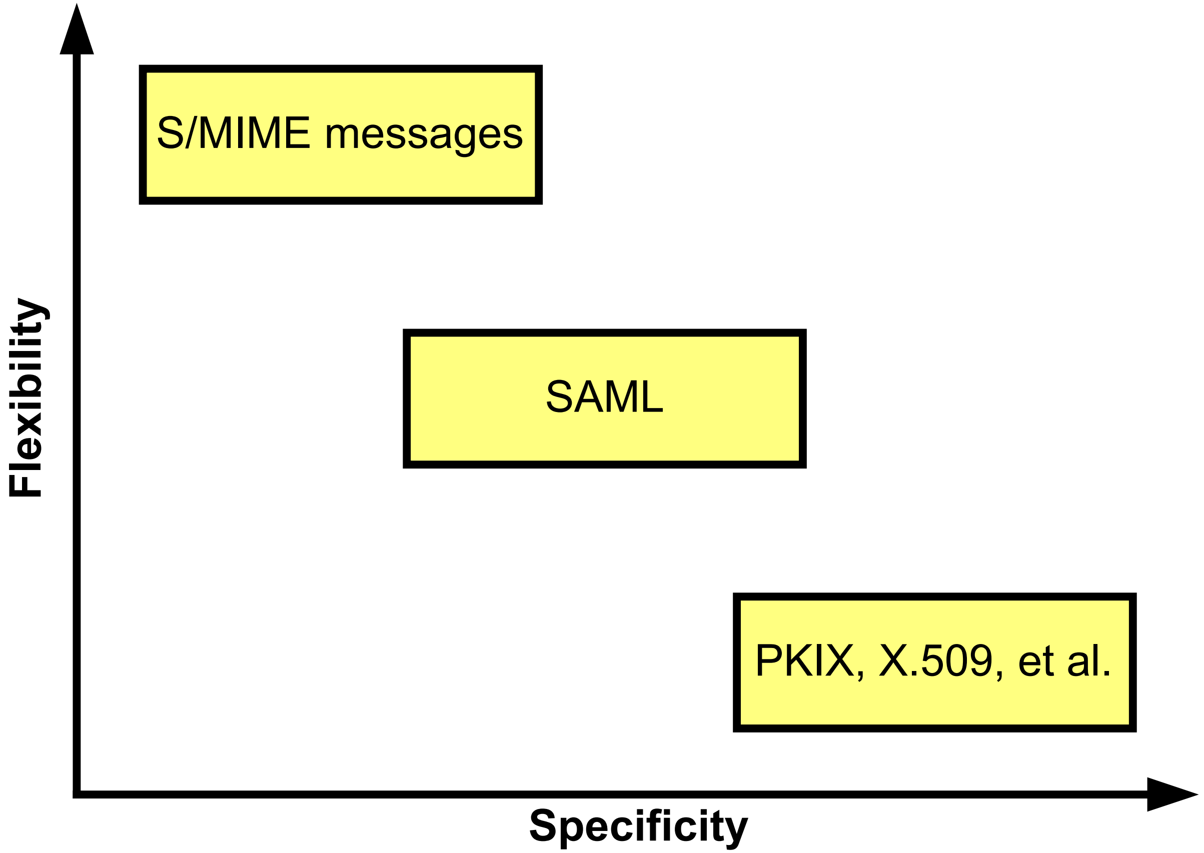
Agenda

- The problem space
- SAML concepts
  - SAML in a nutshell
  - SAML assertions and their producers and consumers
  - Message exchange protocol
  - Bindings and profiles
- Walking through scenarios
- Status of SAML and helpful resources

"SAML on one slide"

- It's an XML-based framework for exchanging security information
  - XML-encoded security "assertions"
  - XML-encoded request/response protocol
  - Rules on using assertions with standard transport and messaging frameworks
- It's an emerging OASIS standard
  - Vendors *and* users are involved
  - Codifies current system outputs rather than inventing new technology

SAML compared to existing security frameworks



XML-related security standards work

- XML Signature
  - SAML builds this in for digitally signing assertions
- XML Encryption
  - Important for flexibly managing security and privacy risks, e.g., encrypting just the credit card number
- XKMS
  - SAML traffic might be secured by XKMS-based PKI, by other PKI, or by other means entirely
- XACML
  - XML-based (and SAML-influenced) access control/ policy language

More XML-related security standards work

- DSML
  - Directory services provided in XML form
- Liberty Alliance
  - Identity solution for SSO of consumers and businesses
- Internet2
  - Higher-education effort to develop advanced network applications and technologies

Industry traction for SAML? For starters…

- Entegrity AssureAccess
- Entrust GetAccess portal
- Netegrity AffiliateMinder
- Oblix NetPoint
- RSA Security Cleartrust
- Sun ONE Identity Server
- Systinet WASP Secure Identity
- JSR 155 in the Java Community Process
- Portions of Internet2

Agenda

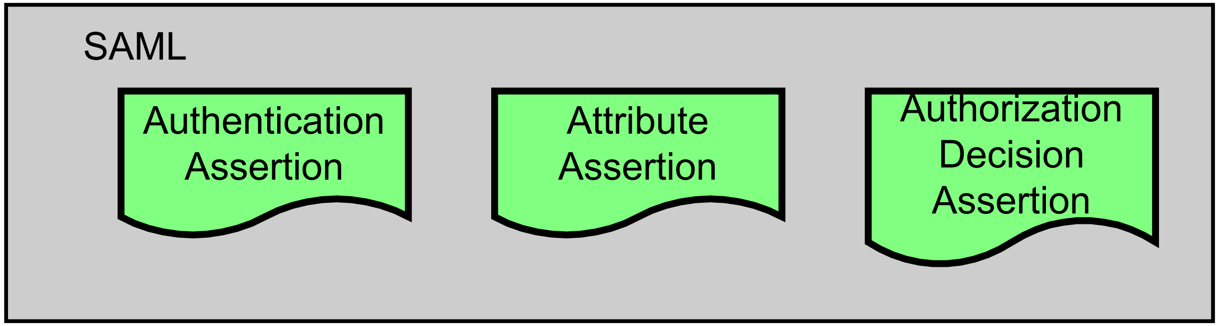
- The problem space
- SAML concepts
  - SAML in a nutshell
  - SAML assertions and their producers and consumers
  - Message exchange protocol
  - Bindings and profiles
- Walking through scenarios
- Status of SAML and helpful resources

SAML assertions

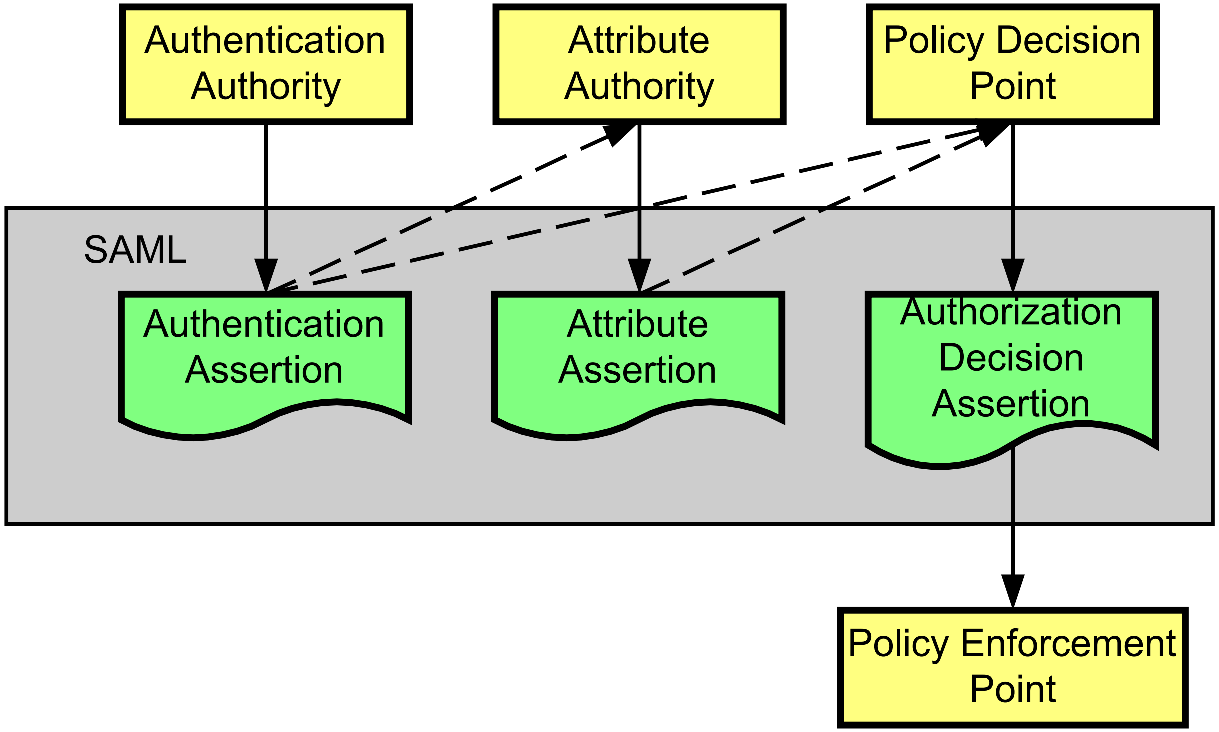
- An assertion is a declaration of fact, according to someone
- SAML assertions are compounds of one or more of three kinds of “statement” about a “subject” (human or program):
  - Authentication
  - Attribute
  - Authorization decision
- They can be digitally signed
- You can extend SAML to make your own kinds of assertions and statements

Model for producing and consuming assertions

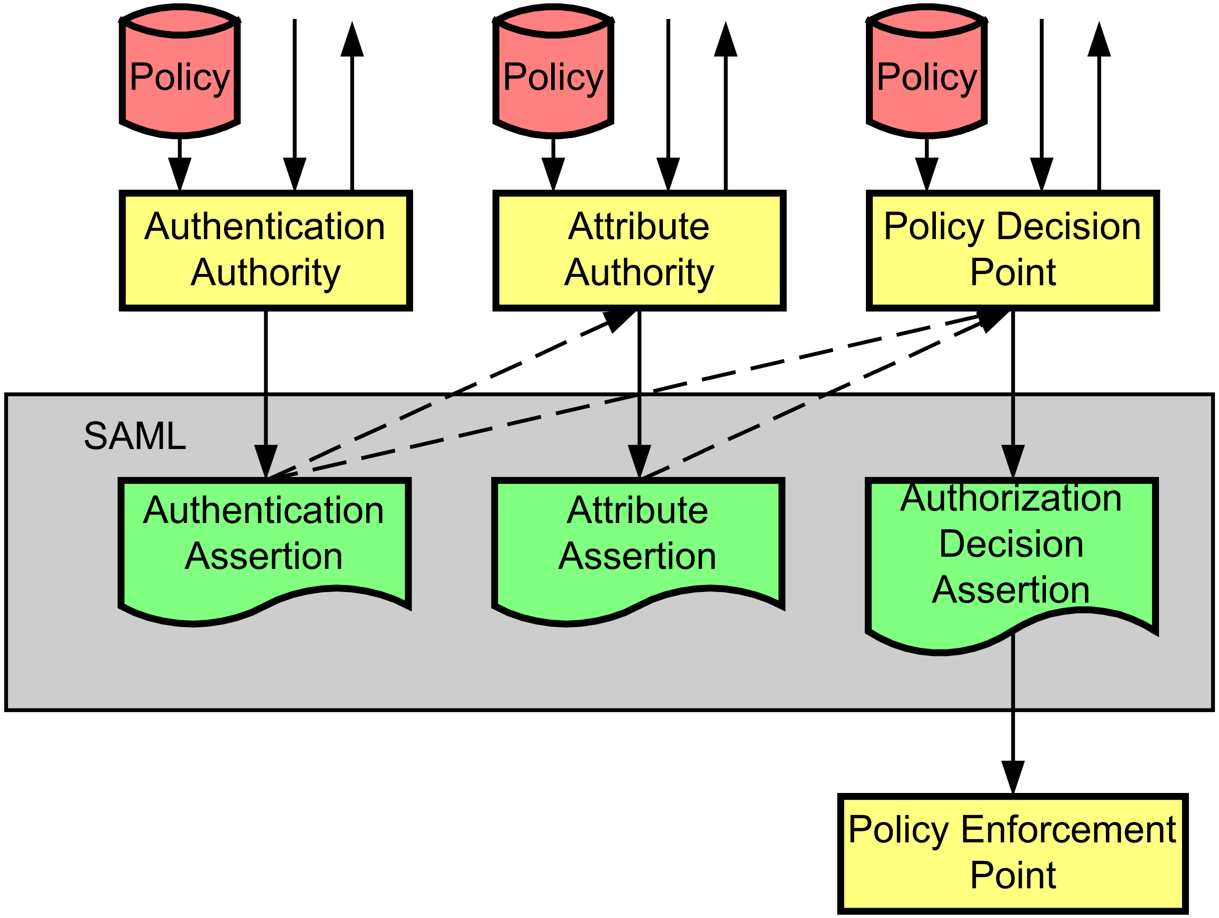
Model for producing and consuming assertions



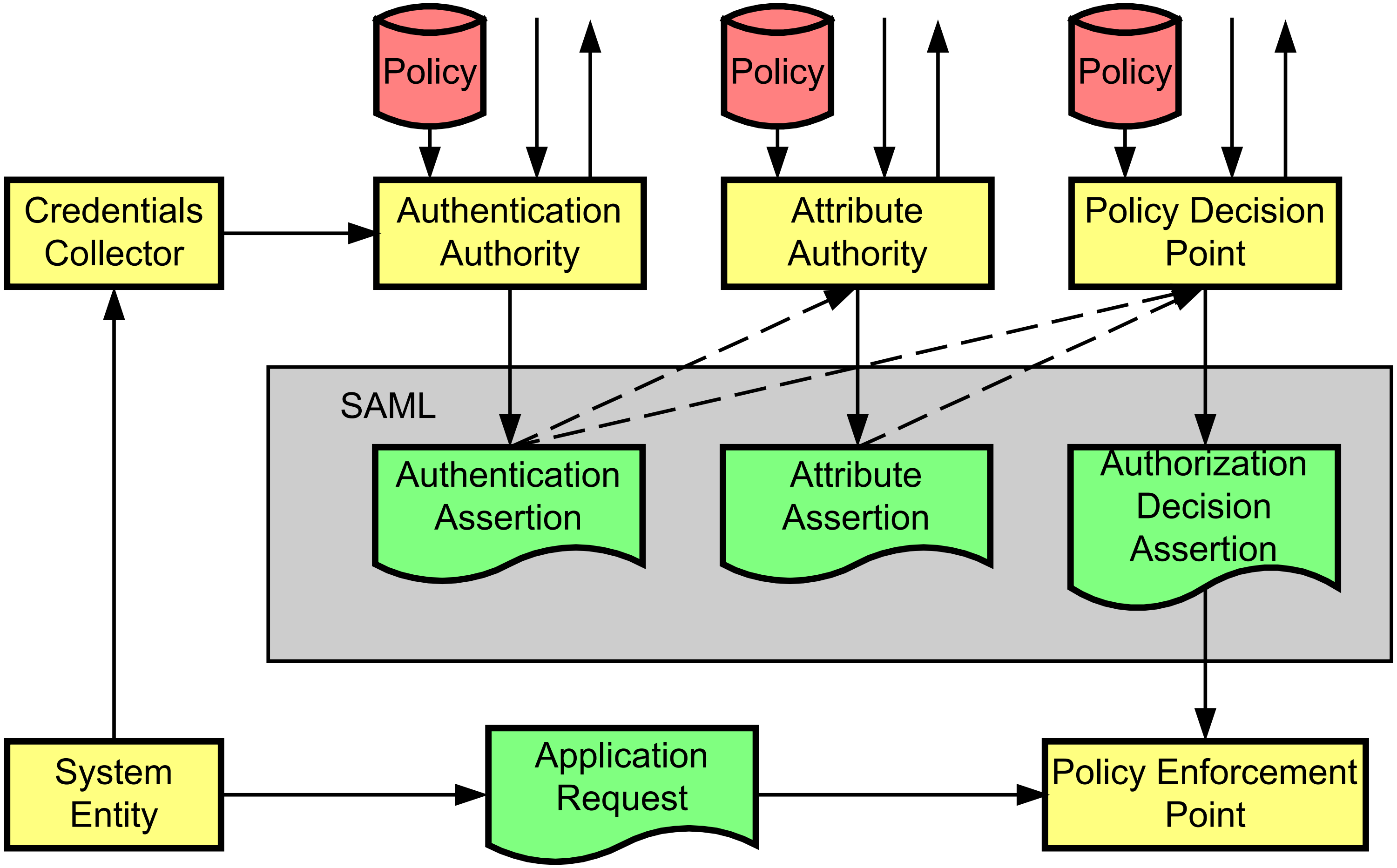
Model for producing and consuming assertions



Model for producing and consuming assertions



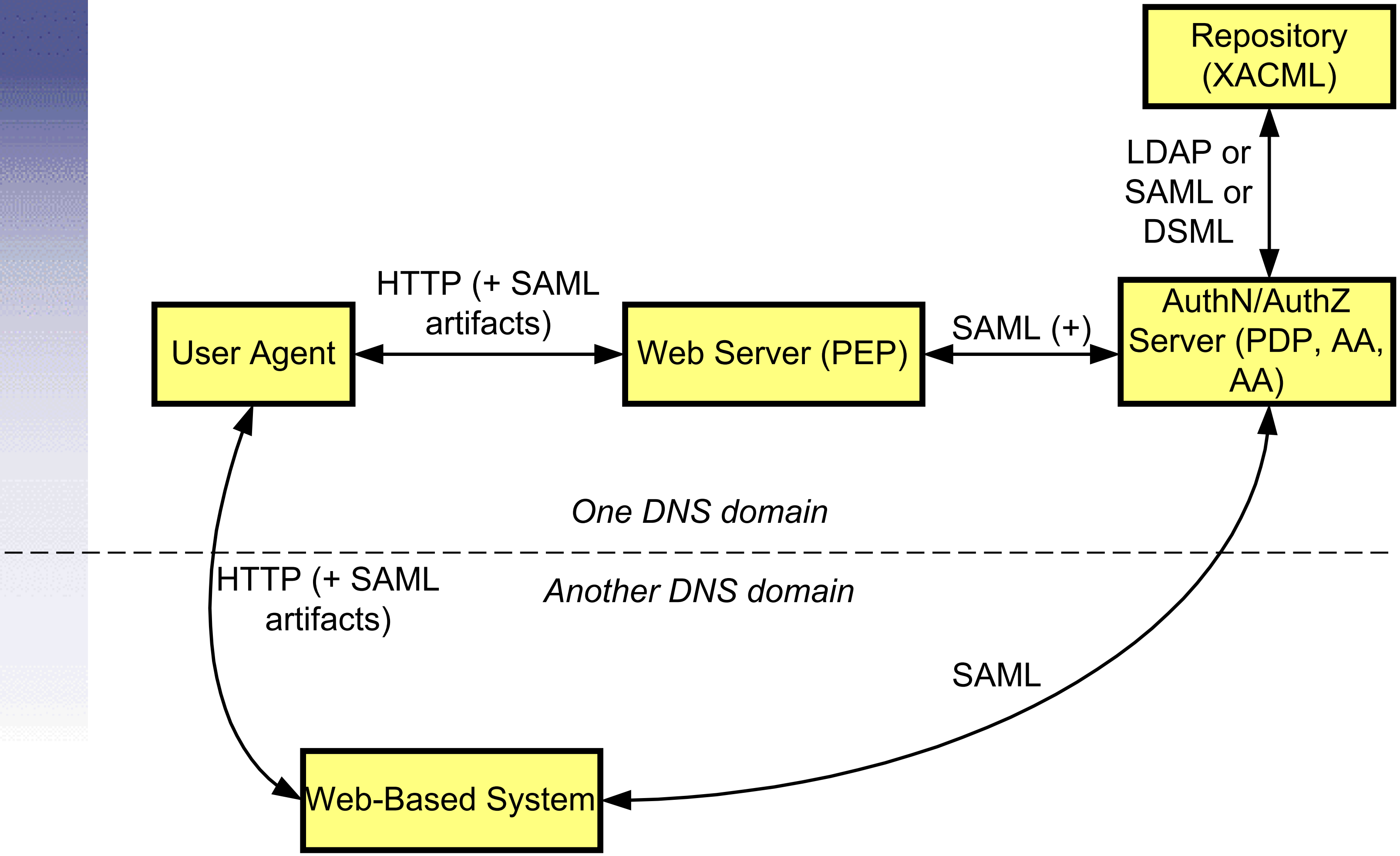
Model for producing and consuming assertions



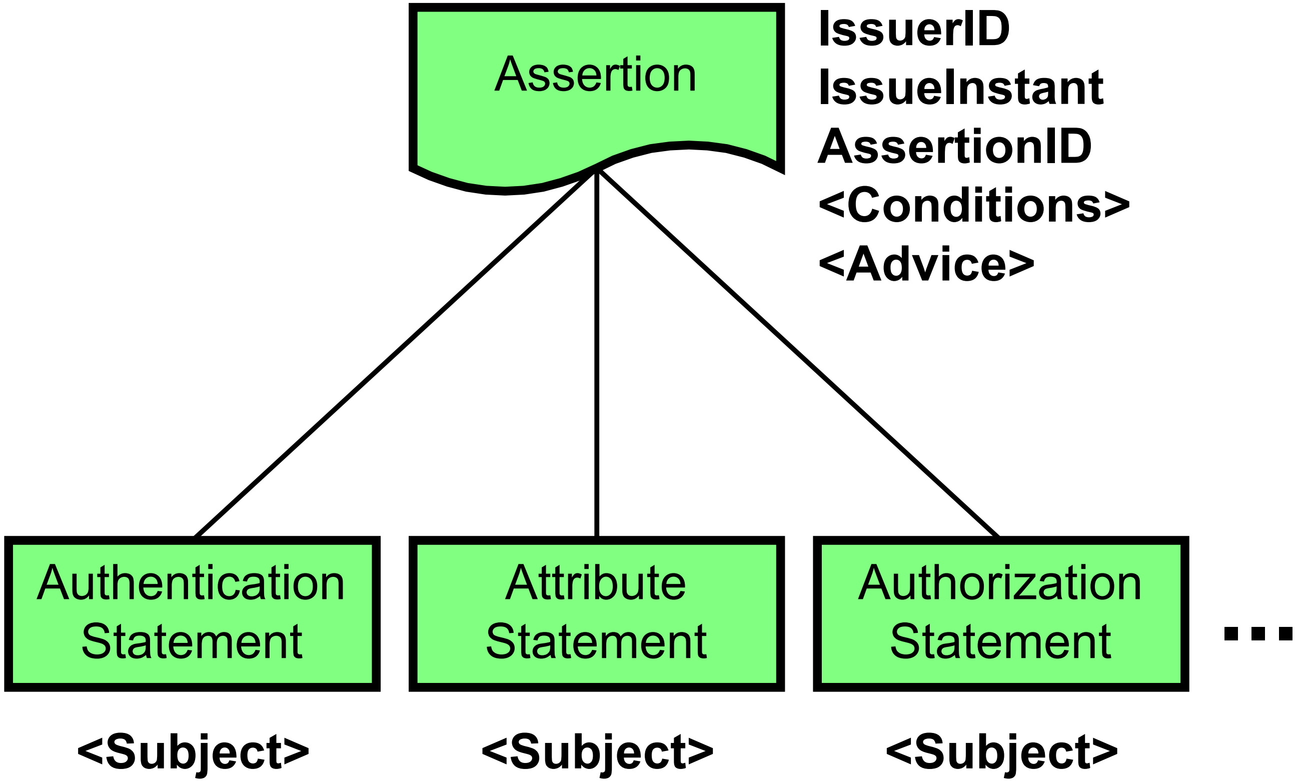
The real world is more complex

- In practice, multiple kinds of authorities may reside in a single software system
  - SAML allows, but doesn’t require, total federation of these jobs
- Also, the arrows may not reflect information flow in real life
  - The order of assertion types is insignificant
  - Information can be pulled or pushed
  - Not all assertions are always produced
  - Not all potential consumers (clients) are shown

A possible deployment architecture



Statements in an assertion share some information



Example common information for an assertion

```
<saml:Assertion
  MajorVersion=“1” MinorVersion=“0”
  AssertionID=“128.9.167.32.12345678”
  Issuer=“Smith Corporation“
  IssueInstant=“2001-12-03T10:02:00Z”>
  <saml:Conditions
    NotBefore=“2001-12-03T10:00:00Z”
    NotOnOrAfter=“2001-12-03T10:05:00Z”>
    <saml:AudienceRestrictionCondition>
      <saml:Audience>…URI…</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:Advice>
    …a variety of elements can go here…
  </saml:Advice>
  …statements go here…
</saml:Assertion>
```

Authentication statement

- An issuing authority asserts that subject S was authenticated by means M at time T
- Targeted towards SSO uses
- **Caution:** Actually checking or revoking of credentials is not in scope for SAML!
- It merely lets you link back to acts of authentication that took place previously

Example assertion with authentication statement

```
<saml:Assertion …>
  <saml:AuthenticationStatement
    AuthenticationMethod=“…URI…”
    AuthenticationInstant=“2001-12-03T10:02:00Z”>
    <saml:Subject>
      <saml:NameIdentifier
        Format=“#emailAddress”>joeuser@smithco.com
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>…URI…
        </saml:ConfirmationMethod>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
 </saml:Assertion>
```

Attribute statement

- An issuing authority asserts that subject S is associated with attributes A, B, … with values “a”, “b”, “c”…
- Useful for distributed transactions and authorization services
- Typically this would be gotten from an LDAP repository
  - “john.doe” in “example.com”
  - is associated with attribute “Department”
  - with value “Human Resources”

Example assertion with attribute statement

```
<saml:Assertion …>
  <saml:AttributeStatement>
    <saml:Subject>…</saml:Subject>
    <saml:Attribute
      AttributeName=“PaidStatus”
      AttributeNamespace=“http://smithco.com”>
      <saml:AttributeValue>
        PaidUp
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeName=“CreditLimit”
      AttributeNamespace=“http://smithco.com”>
      <saml:AttributeValue xsi:type=“my:type”>
        <my:amount currency=“USD”>500.00
        </my:amount>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Authorization decision statement

- An issuing authority decides whether to grant the request by subject S for access type A to resource R given evidence E
- Useful for distributed transactions and authorization services
- The subject could be a human or a program
- The resource could be a web page or a web service, for example

Example assertion with authorization decision statement

```
<saml:Assertion …>
  <saml:AuthorizationStatement
    Decision=“Permit”
    Resource=“http://jonesco.com/rpt_12345.htm”>
    <saml:Subject>…</saml:Subject>
    <saml:Action Namespace=
“urn:oasis:names:tc:SAML:1.0:action:rwedc”>Read
    </saml:Action>
  </saml:AuthorizationStatement>
</saml:Assertion>
```

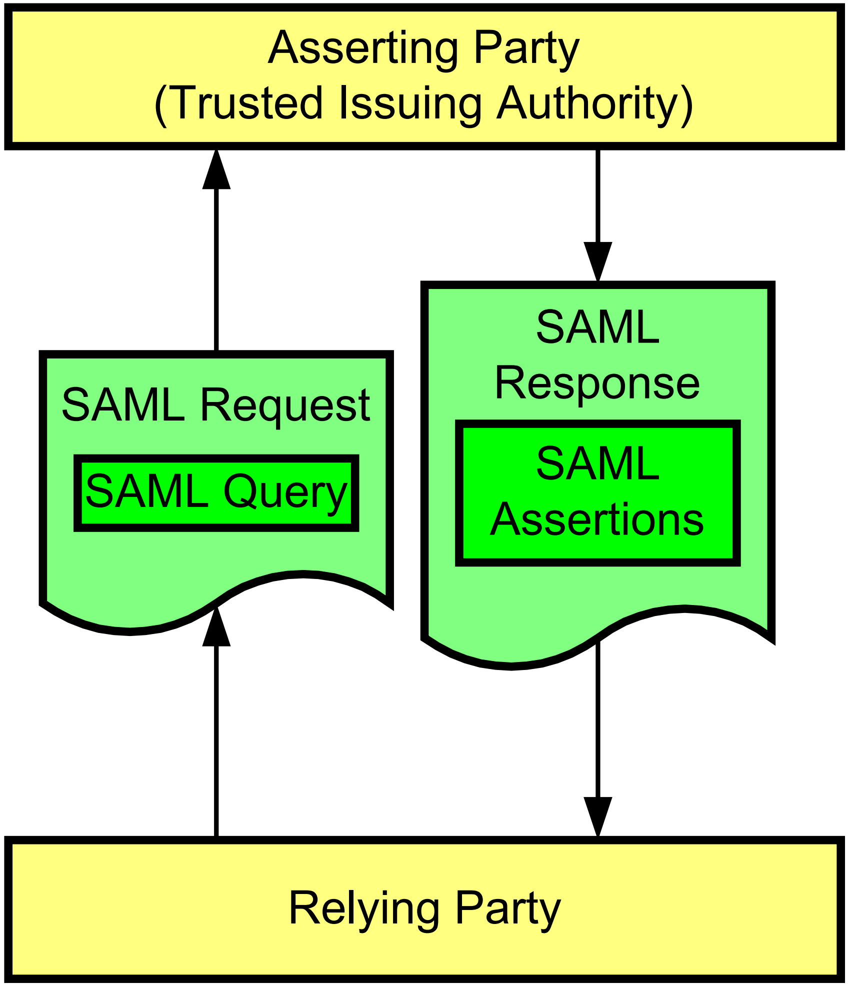
Extension points in the SAML assertion schema

- Assertion
- *Statement*
  - *SubjectStatement*
    - AuthenticationStatement
    - AttributeStatement
    - AuthorizationDecisionStatement
- (There are no final types or blocked elements)
- Extension may come at the price of interoperability

Agenda

- The problem space
- SAML concepts
  - SAML in a nutshell
  - SAML assertions and their producers and consumers
  - Message exchange protocol
  - Bindings and profiles
- Walking through scenarios
- Status of SAML and helpful resources

SAML protocol for getting assertions



Assertions are normally provided in a SAML response

- Existing tightly coupled environments may need to use their own protocol
  - They can use assertions without the rest of the structure
- The full benefit of SAML will be realized where parties with no direct knowledge of each other can interact
  - Via a third-party introduction

Requests can take several forms

- You can query for specific kinds of assertion/statement
  - Authentication query
  - Attribute query
  - Authorization decision query
- You can ask for an assertion with a particular ID
  - By providing an ID reference
  - By providing a SAML “artifact”

Authentication query

- “Please provide the authentication information for this subject, if you have any”
- It is assumed that the requester and responder have a trust relationship
  - They are talking about the same subject
  - The response with the assertion is a “letter of introduction” for the subject

Example request with authentication query

```
<samlp:Request
 MajorVersion=“1” MinorVersion=“0”
  RequestID=“128.14.234.20.12345678”
  IssueInstant=“2001-12-03T10:02:00Z”>
  <samlp:RespondWith>saml:AuthenticationStatement
  <ds:Signature>…</ds:Signature>
  <samlp:AuthenticationQuery>
    <saml:Subject>…</saml:Subject>
  </samlp:AuthenticationQuery>
</samlp:Request>
```

Attribute query

- “Please provide information on the listed attributes for this subject”
- If you don’t list any attributes, you’re asking for all available ones
- If the requester is denied access to some of the attributes, only the allowed attributes would be returned
  - This situation is indicated in the status code of the response

Example request with attribute query

```
<samlp:Request … >
  <samlp:AttributeQuery>
    <saml:Subject>…</saml:Subject>
    <saml:AttributeDesignator
      AttributeName=“PaidStatus”
      AttributeNamespace=“http://smithco.com”/>
  </samlp:AttributeQuery>
</samlp:Request>
```

Authorization decision query

- “Is this subject allowed to access the specified resource in the specified manner, given this evidence?”
- This is a yes-or-no question
  - The answer is not allowed to be “no, but they’re allowed to access these other resources”
  - Or “yes, and they’re also allowed to perform these other actions”

Example authorization decision query

```
<samlp:Request …>
  <samlp:AuthorizationQuery
    Resource=“http://jonesco.com/rpt_12345.htm”>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain=“smithco.com”
        Name=“joeuser” />
    </saml:Subject>
    <saml:Action Namespace=
“urn:oasis:names:tc:SAML:1.0:action:rwedc”>Read
    </saml:Action>
    <saml:Evidence>
    <saml:Assertion>…</saml:Assertion>
    </saml:Evidence>
  </samlp:AuthorizationQuery>
</samlp:Request>
```

Responses just contain a set of assertions

- One or more assertions can be returned with status information
- If something went wrong, no assertions are returned, just status
  - Status information can have a complex structure
- Responses are expected to be signed

Example response

```
<samlp:Response
 MajorVersion=“1” MinorVersion=“0”
  ResponseID=“128.14.234.20.90123456”
  InResponseTo=“128.14.234.20.12345678”
  IssueInstant=“2001-12-03T10:02:00Z”
  Recipient=“…URI…”>
  <samlp:Status>…</samlp:Status>
  <saml:Assertion
    MajorVersion=“1” MinorVersion=“0”
    AssertionID=“128.9.167.32.12345678”
    Issuer=“Smith Corporation">
    <saml:Conditions
      NotBefore=“2001-12-03T10:00:00Z”
      NotAfter=“2001-12-03T10:05:00Z” />
    <saml:AuthenticationStatement …>…
    </saml:AuthenticationStatement>
  </saml:Assertion>
</samlp:Response>
```

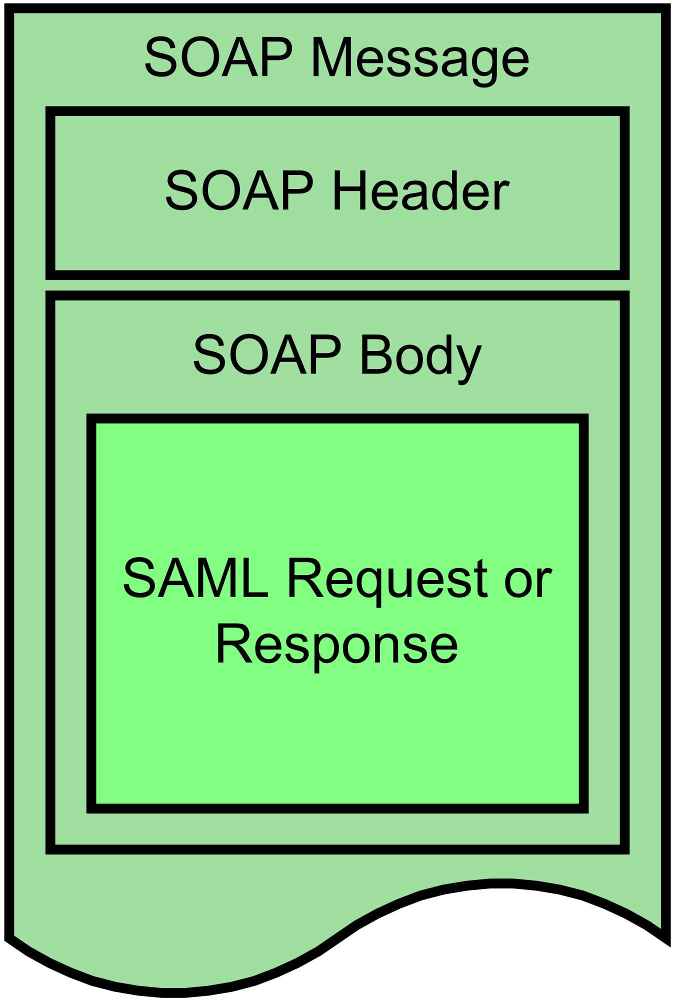
Agenda

- The problem space
- SAML concepts
  - SAML in a nutshell
  - SAML assertions
  - Producers and consumers of assertions
  - Message exchange protocol
  - Bindings and profiles
- Walking through scenarios
- Status of SAML and helpful resources

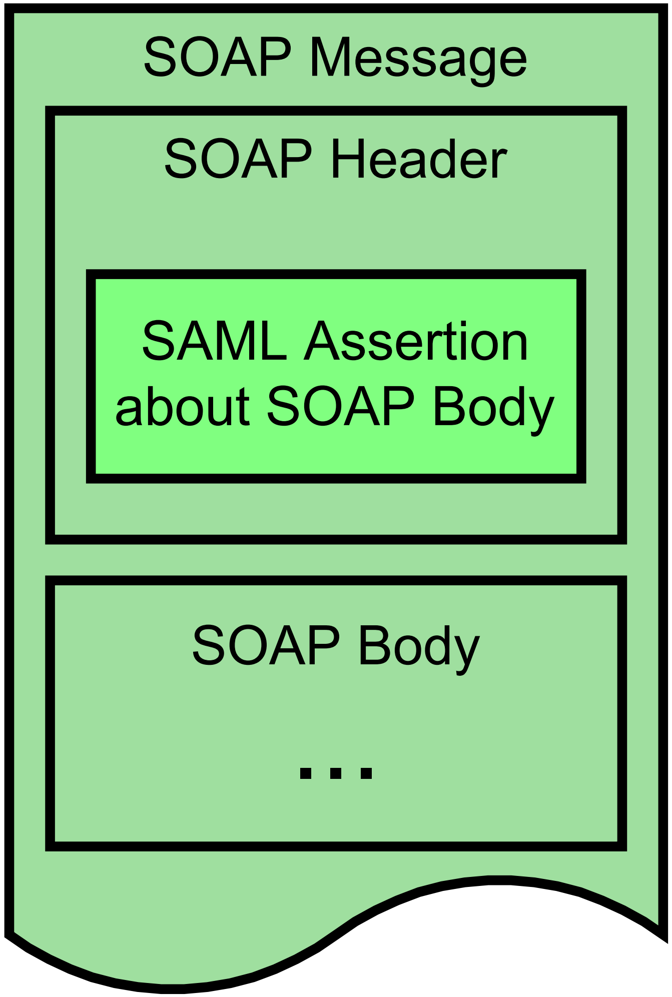
Bindings and profiles connect SAML with the wire

- This is where SAML itself gets made secure
- A “binding” is a way to transport SAML requests and responses
  - SOAP-over-HTTP binding is a baseline
  - Other bindings will follow, e.g., raw HTTP
- A “profile” is a pattern for how to make assertions about other information
  - Two browser profiles for SSO: artifact and POST
  - SOAP profile for securing SOAP payloads

The SOAP-over-HTTP binding



By contrast, the SOAP profile



Web browser profiles

- These profiles assume:
  - A standard commercial browser and HTTP(S)
  - User has authenticated to a local source site
  - Assertion's subject refers implicitly to the user
- When a user tries to access a target site:
  - A tiny authentication assertion reference travels with the request so the real assertion can be dereferenced
  - Or the real assertion gets POSTed

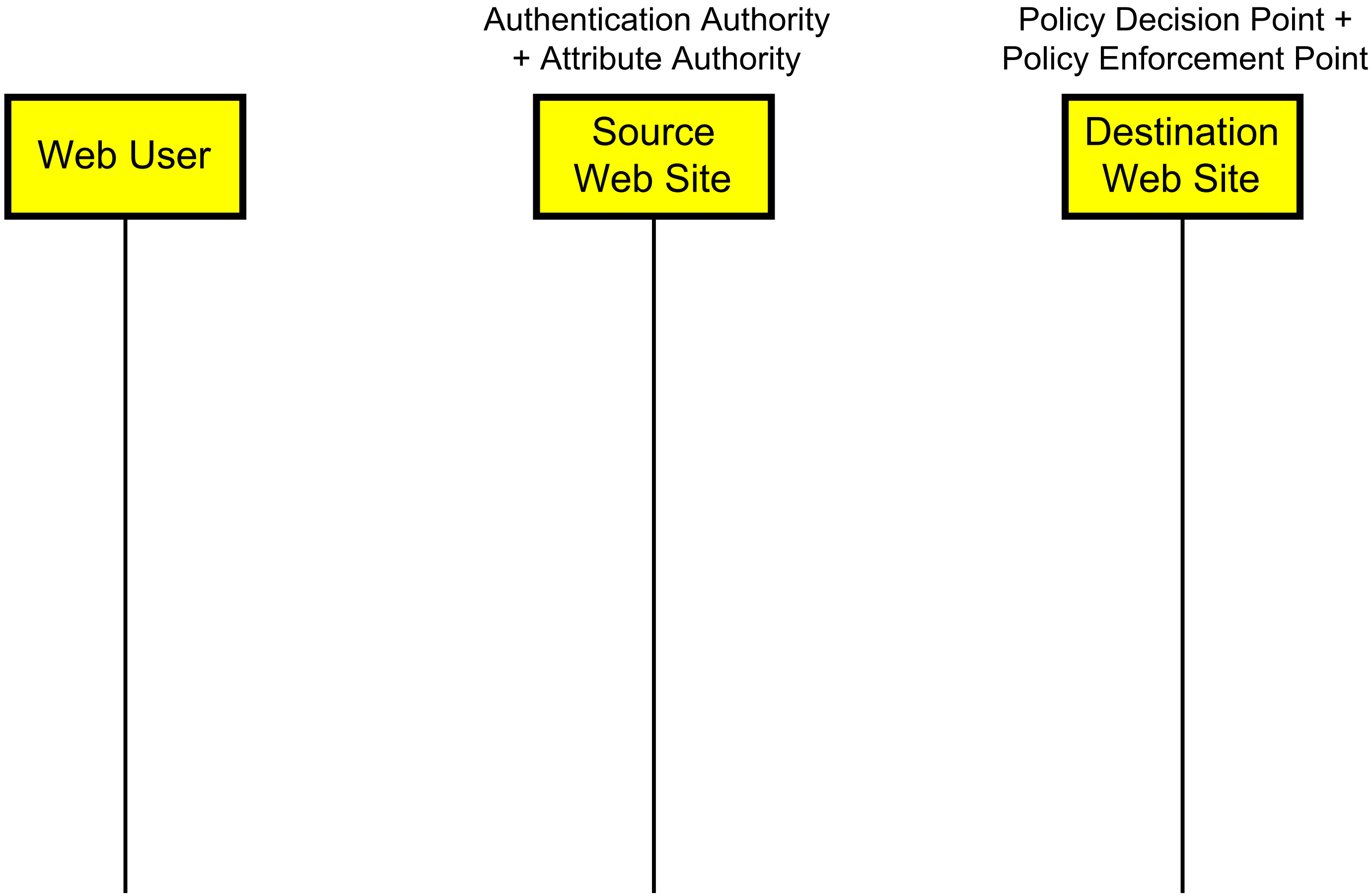
Future bindings and profiles

- The SAML committee will accept and register proposed new bindings and profiles
- Eventually we may standardize these
- Open publishing of these will at least help interoperability in the meantime

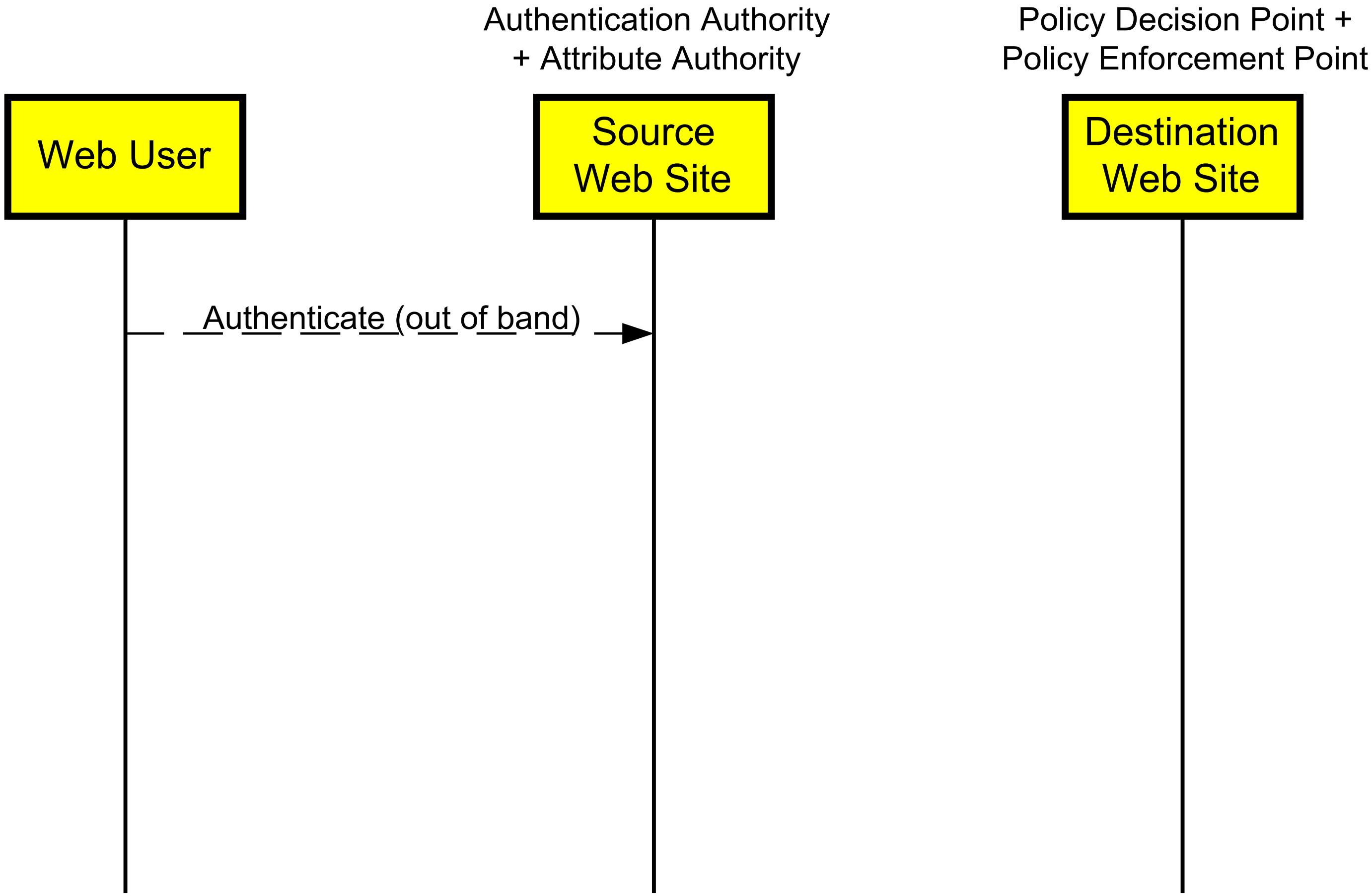
Agenda

- The problem space
- SAML concepts
- Walking through scenarios
  - SSO pull using the browser/artifact profile
  - Back office transaction using the SOAP binding and the SOAP profile
- Status of SAML and helpful resources

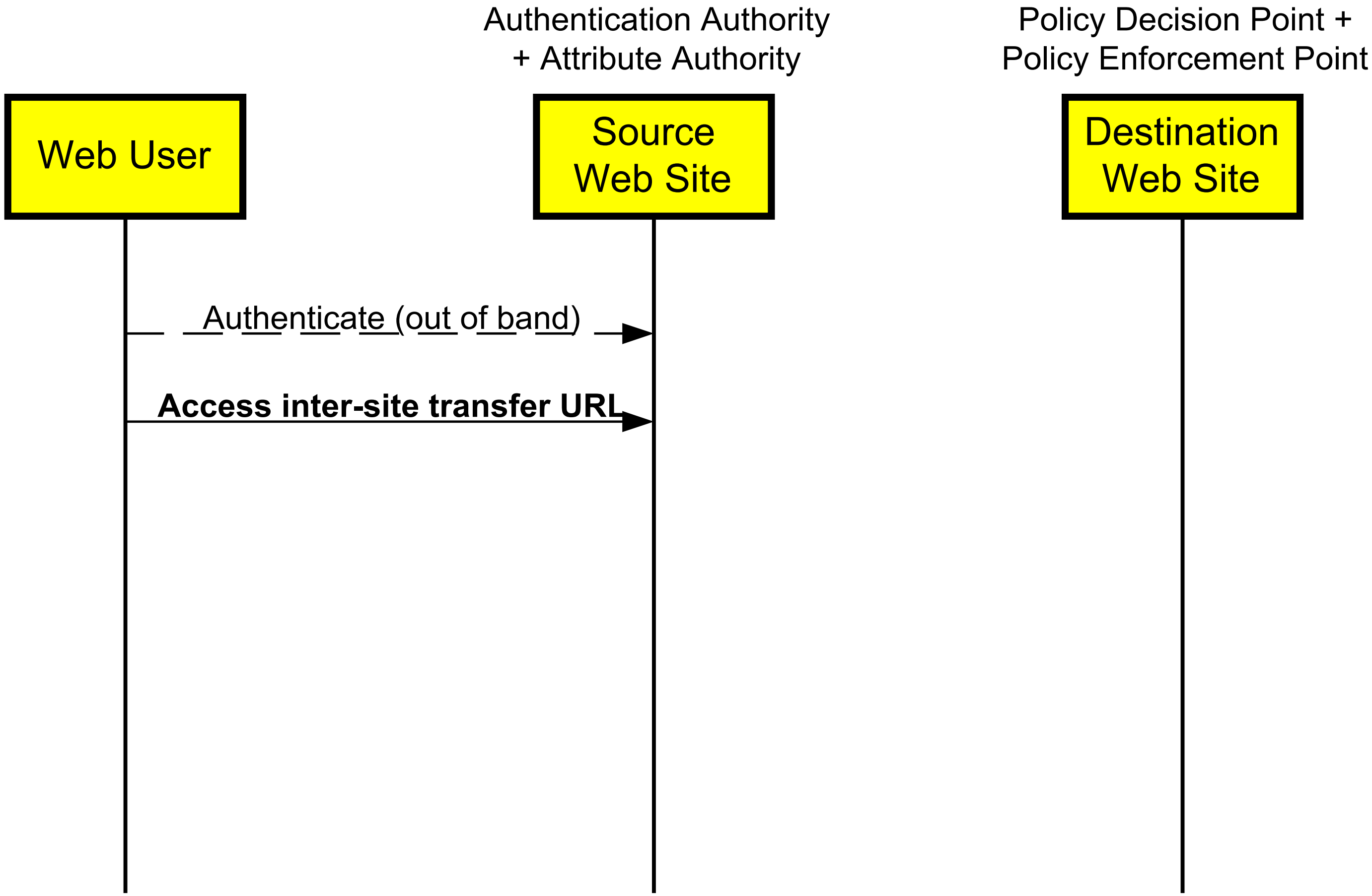
SSO pull scenario



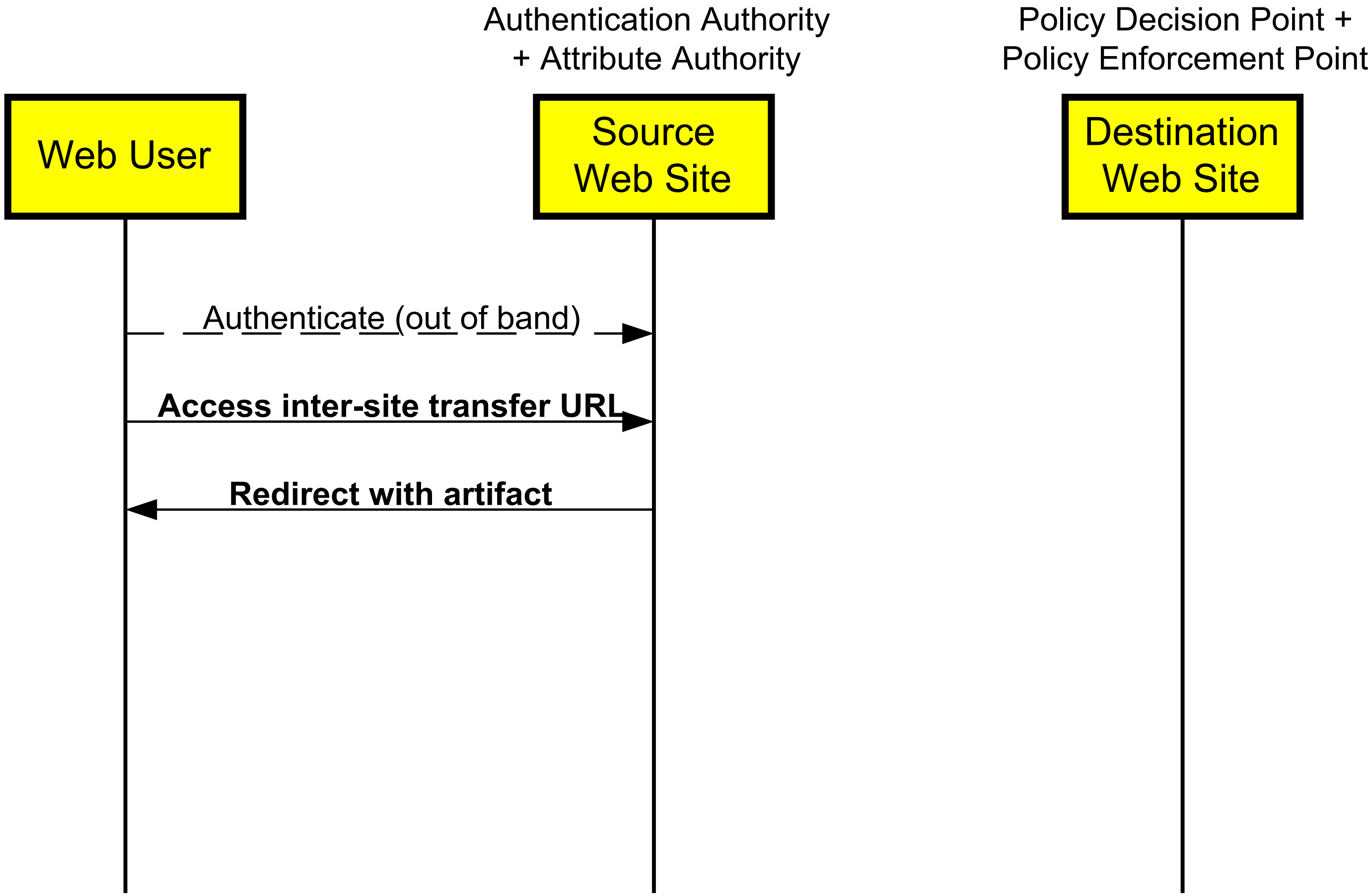
SSO pull scenario



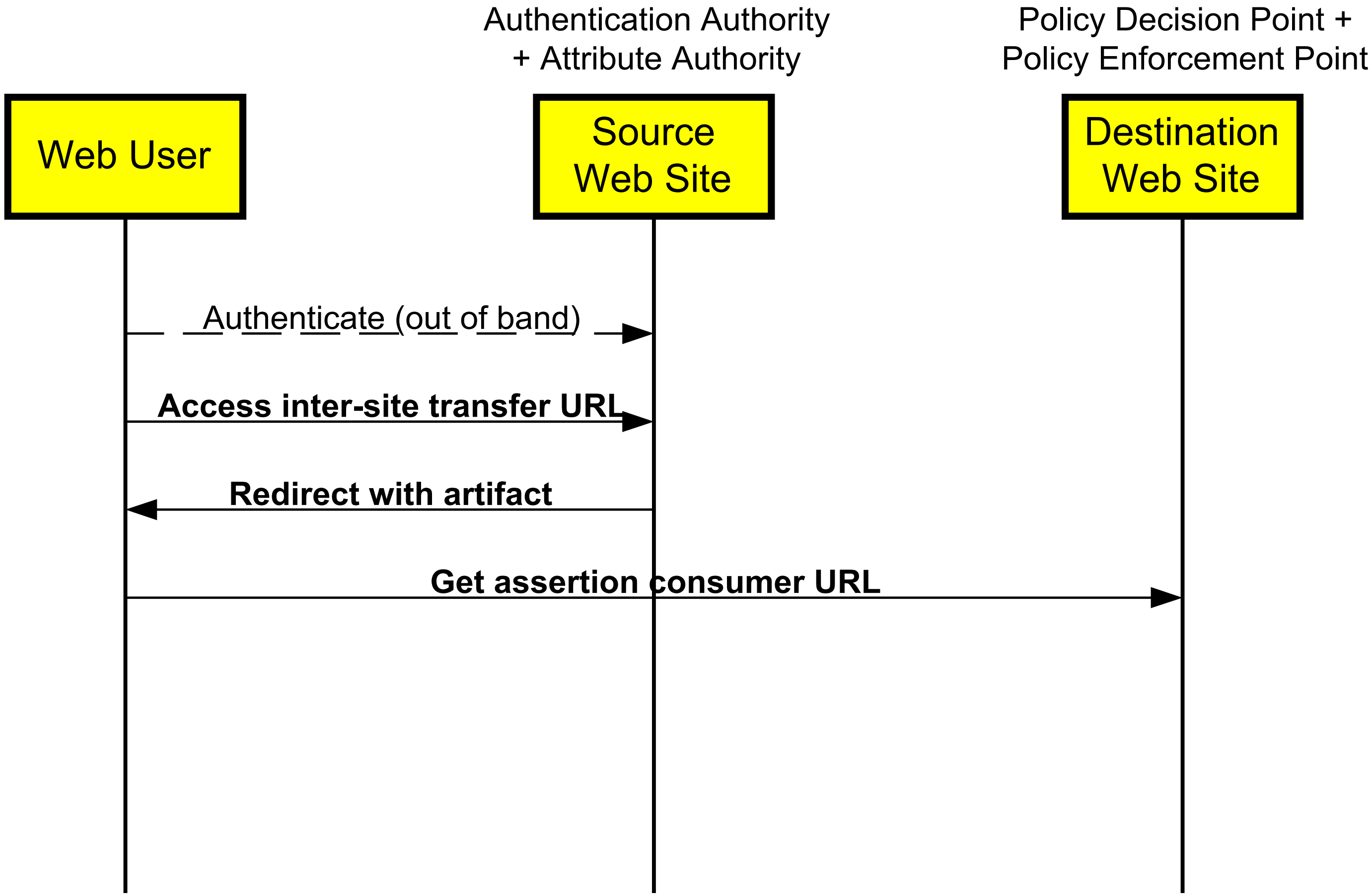
SSO pull scenario



SSO pull scenario

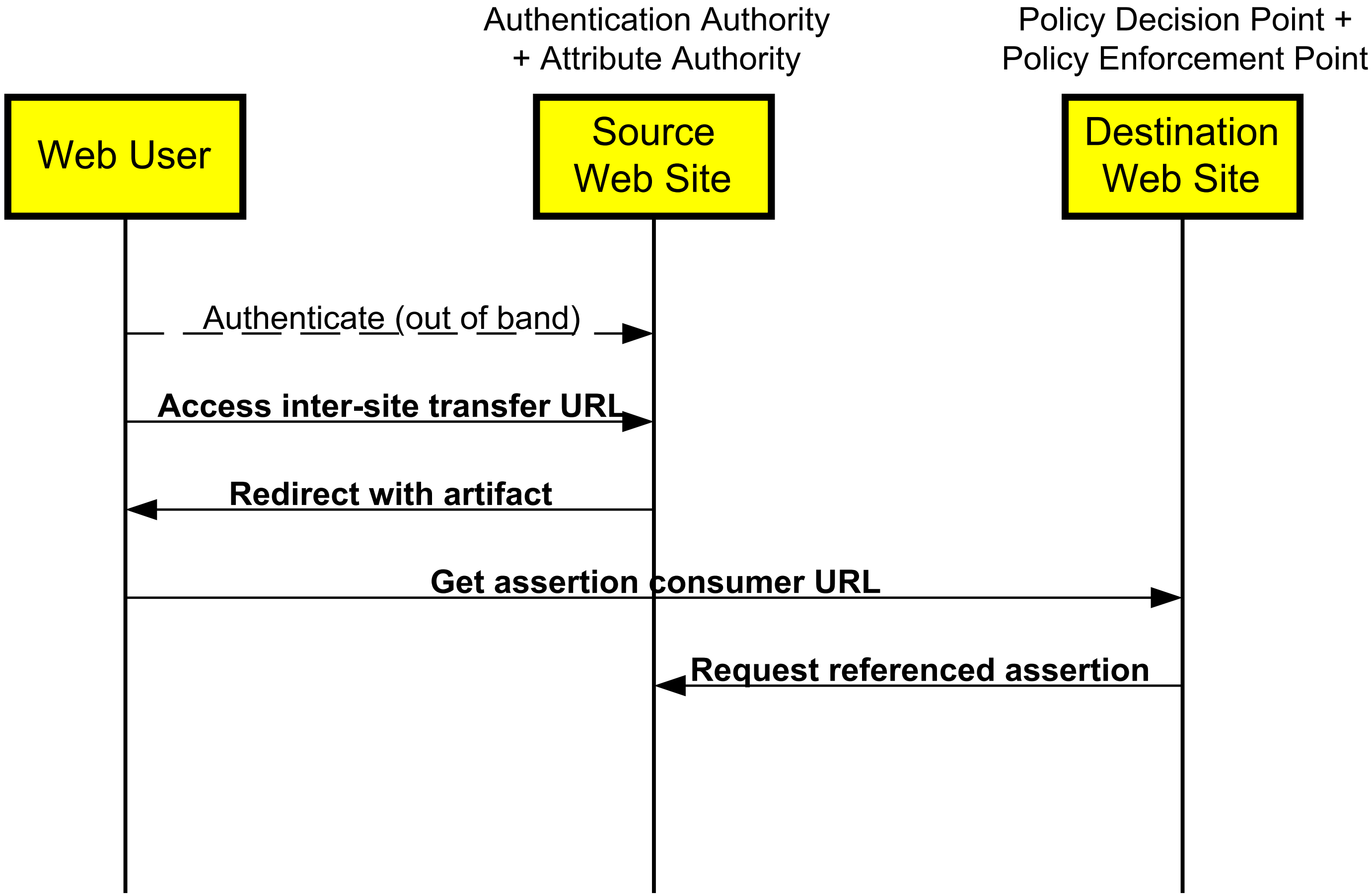


SSO pull scenario

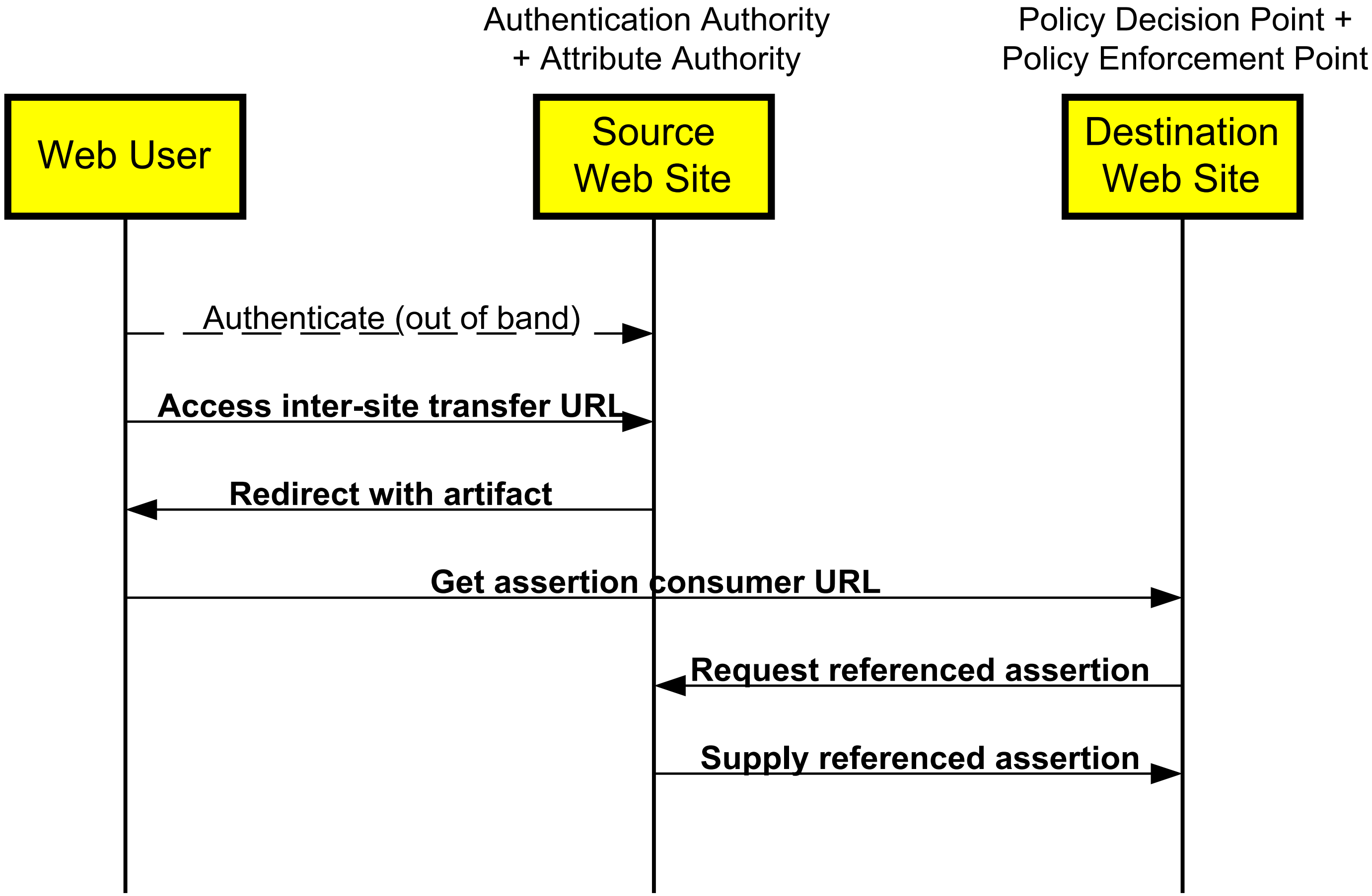


Authentication Authority + Attribute Authority
Policy Decision Point + Policy Enforcement Point
Web User
Source Web Site
Destination Web Site
Authenticate (out of band)
Access inter-site transfer URL
Redirect with artifact
Get assertion consumer URL

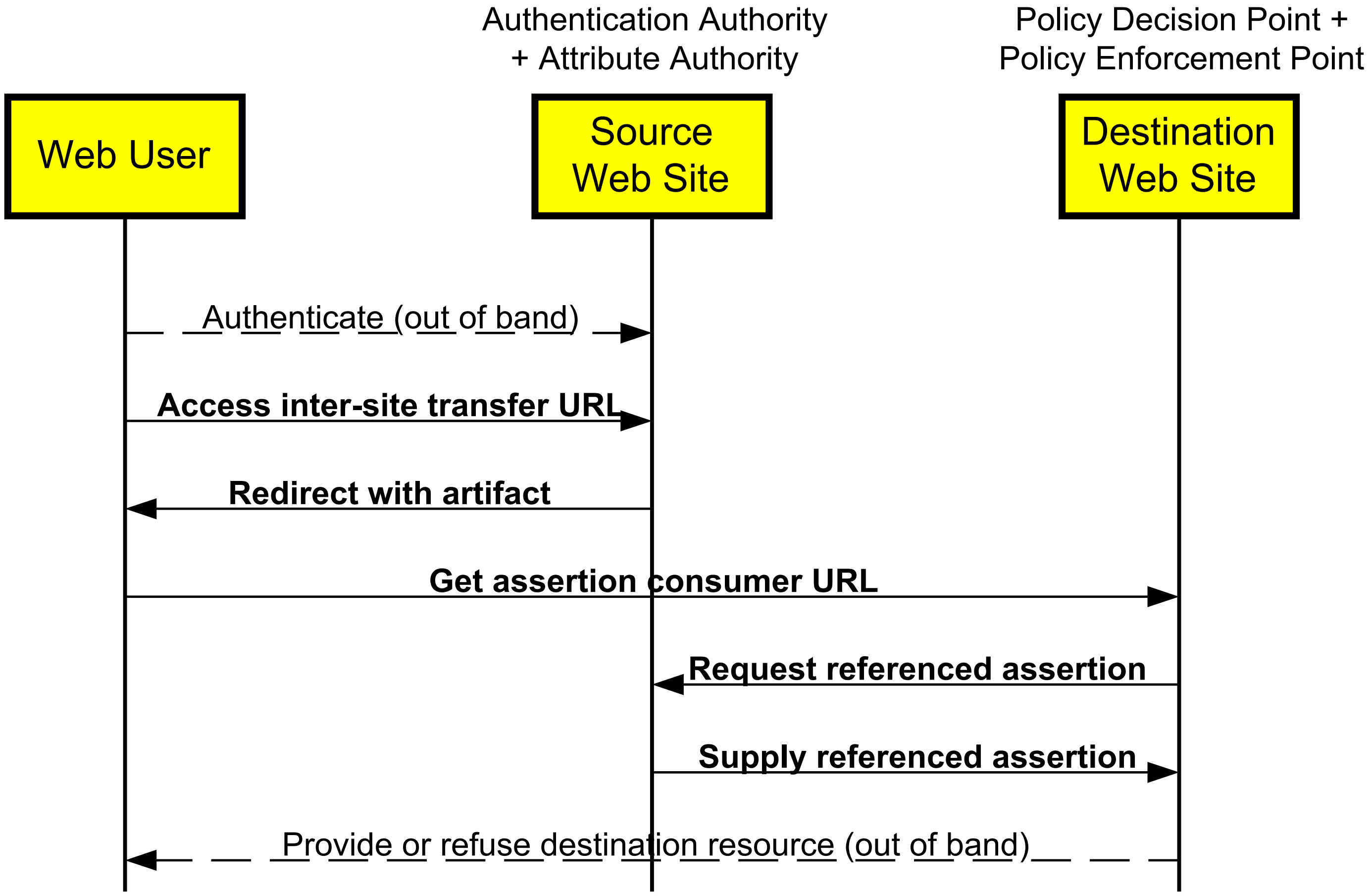
SSO pull scenario



SSO pull scenario



SSO pull scenario


Authentication Authority
+ Attribute Authority
Policy Decision Point +
Policy Enforcement Point
Web User
Source Web Site
Destination Web Site
Authenticate (out of band)
Access inter-site transfer URL
Redirect with artifact
Get assertion consumer URL
Request referenced assertion
Supply referenced assertion
Provide or refuse destination resource (out of band)

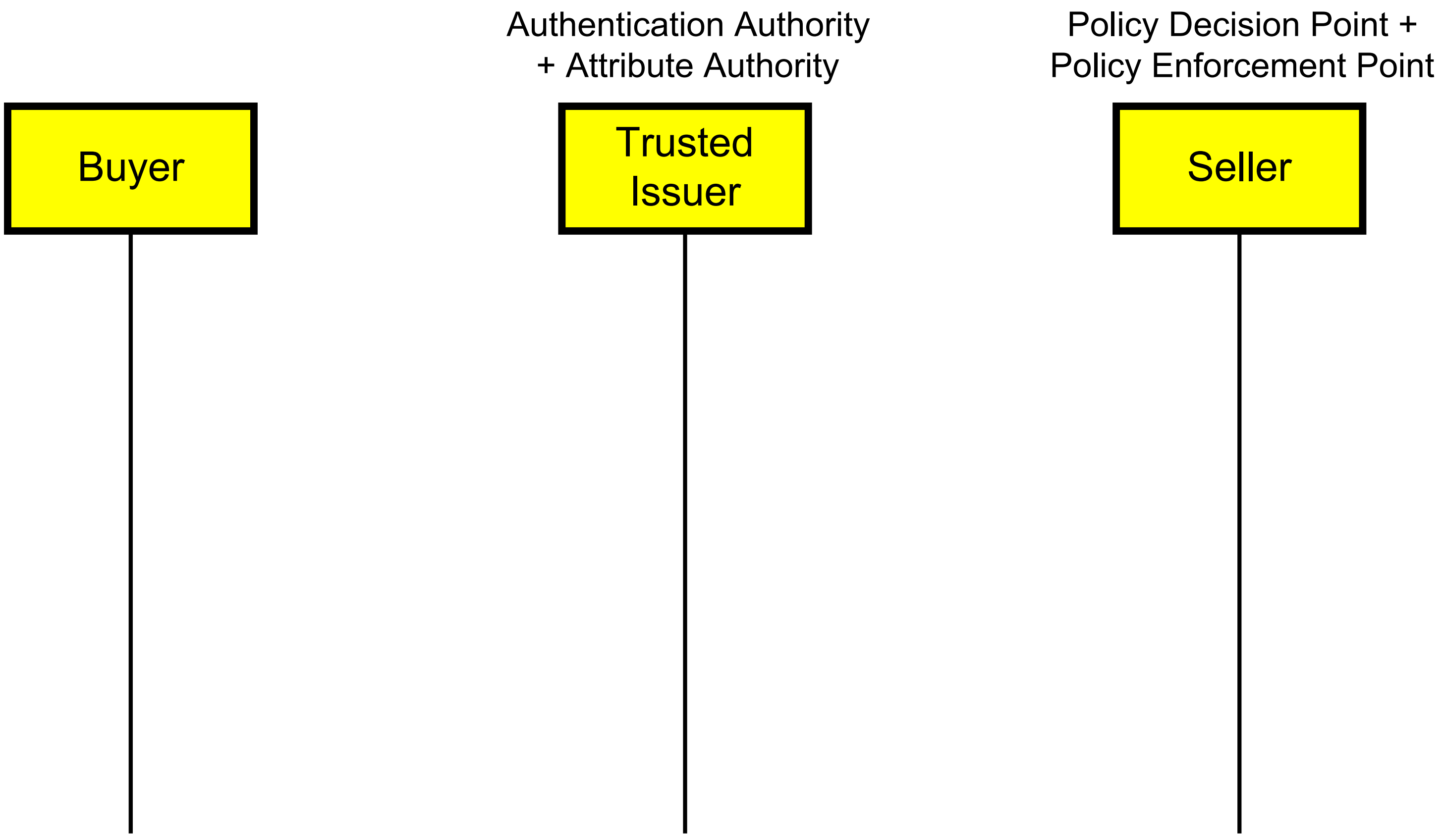
More on the SSO pull scenario

- "Access inter-site transfer URL" step:
  - User is at: `http://smithco.com`
  - Clicks on a link that looks like it will take her to `http://jonesco.com`
  - It really takes her to inter-site transfer URL: `https://smithco.com/intersite?dest=jonesco.com`
- "Redirect with artifact" step:
  - Reference to user's authentication assertion is generated as a SAML "artifact" (8-byte base64 string)
  - User is redirected to assertion consumer URL, with artifact and target attached: `https://jonesco.com?SAMLart=<artifact>`

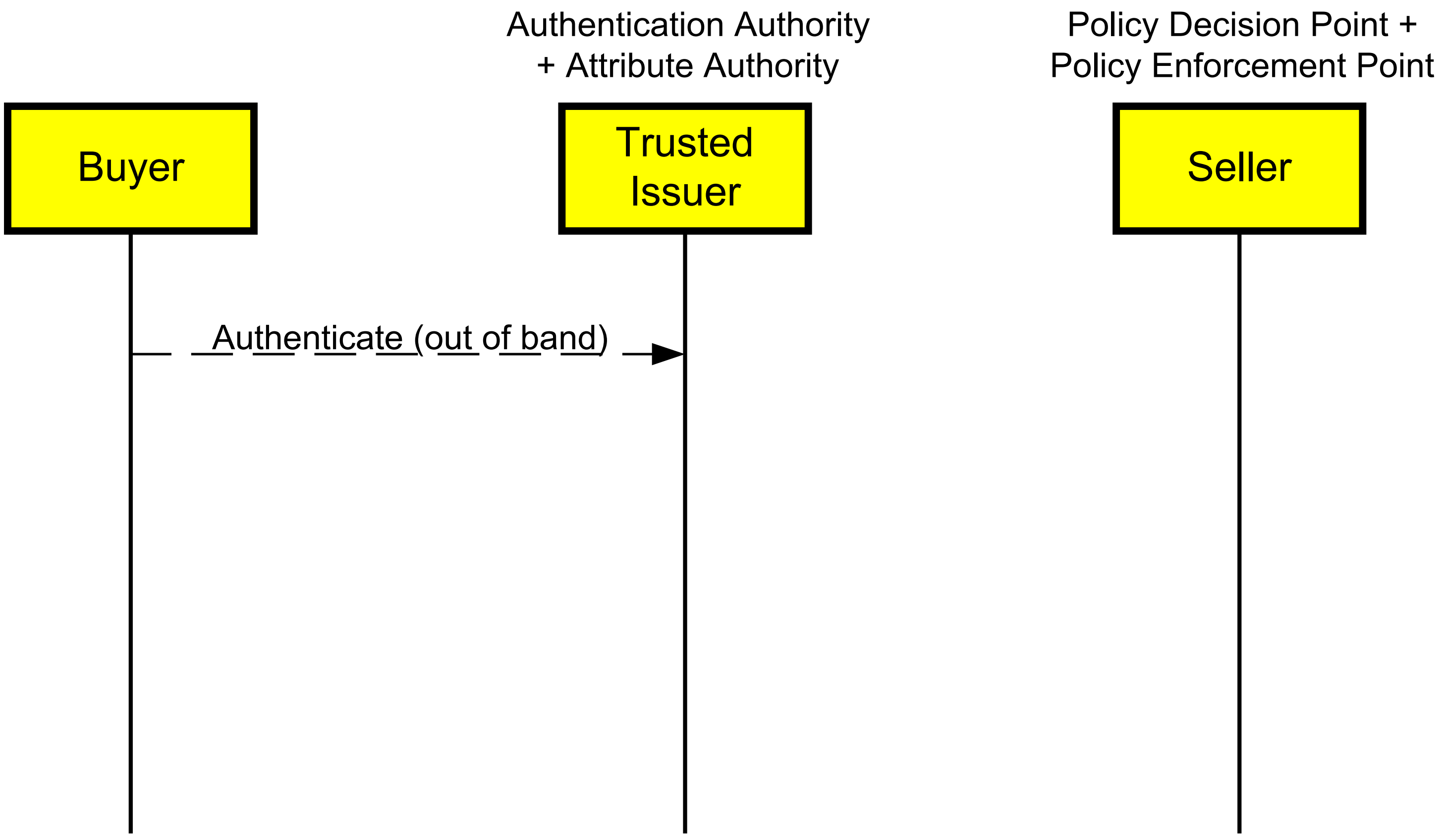
Agenda

- The problem space
- SAML concepts
- Walking through scenarios
  - SSO pull using the web browser profile
  - Distributed transaction using the SOAP binding and the SOAP profile
- Status of SAML and helpful resources

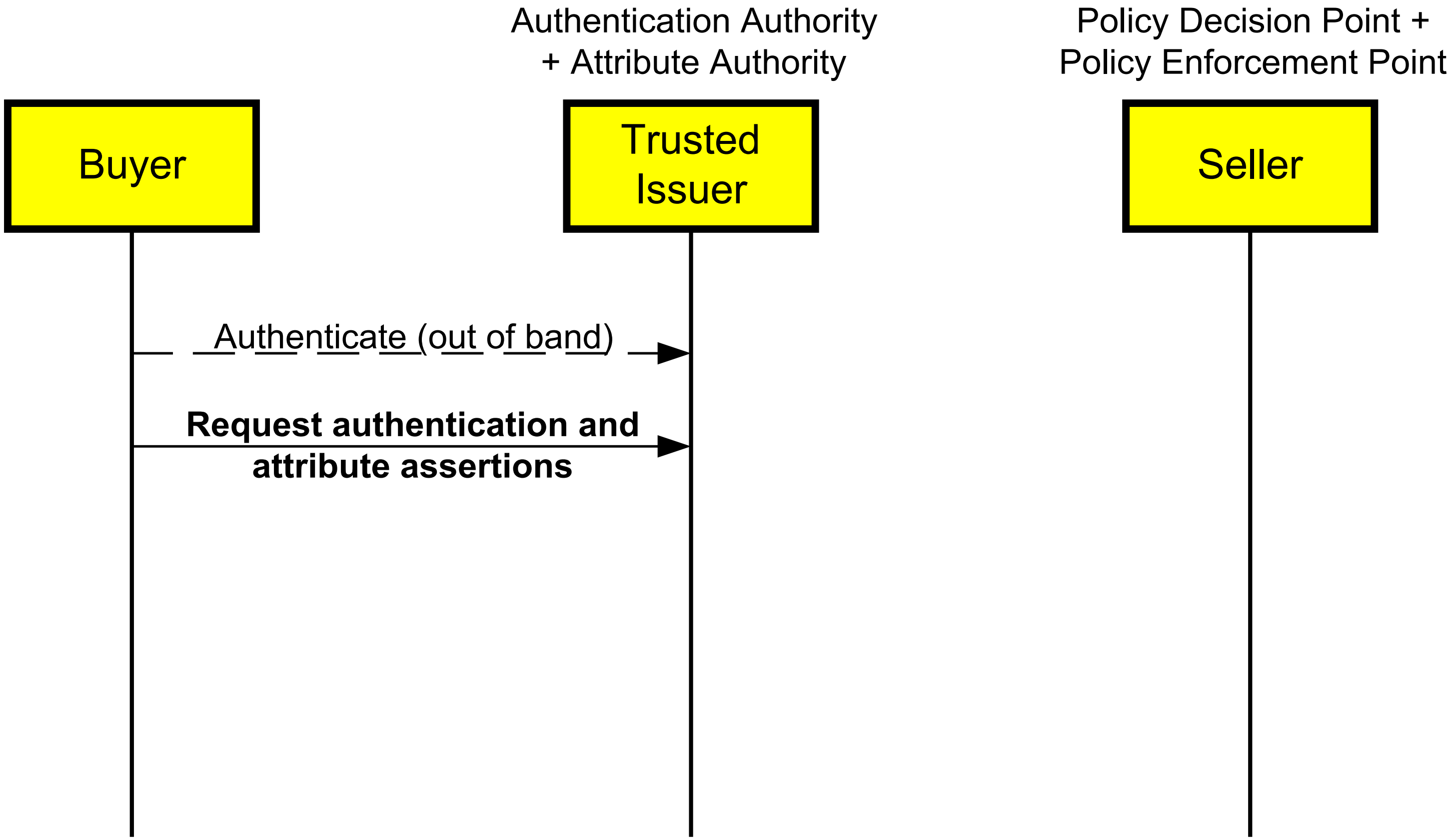
Distributed transaction scenario


Authentication Authority + Attribute Authority
Policy Decision Point + Policy Enforcement Point
Buyer
Trusted Issuer
Seller

Distributed transaction scenario



Distributed transaction scenario

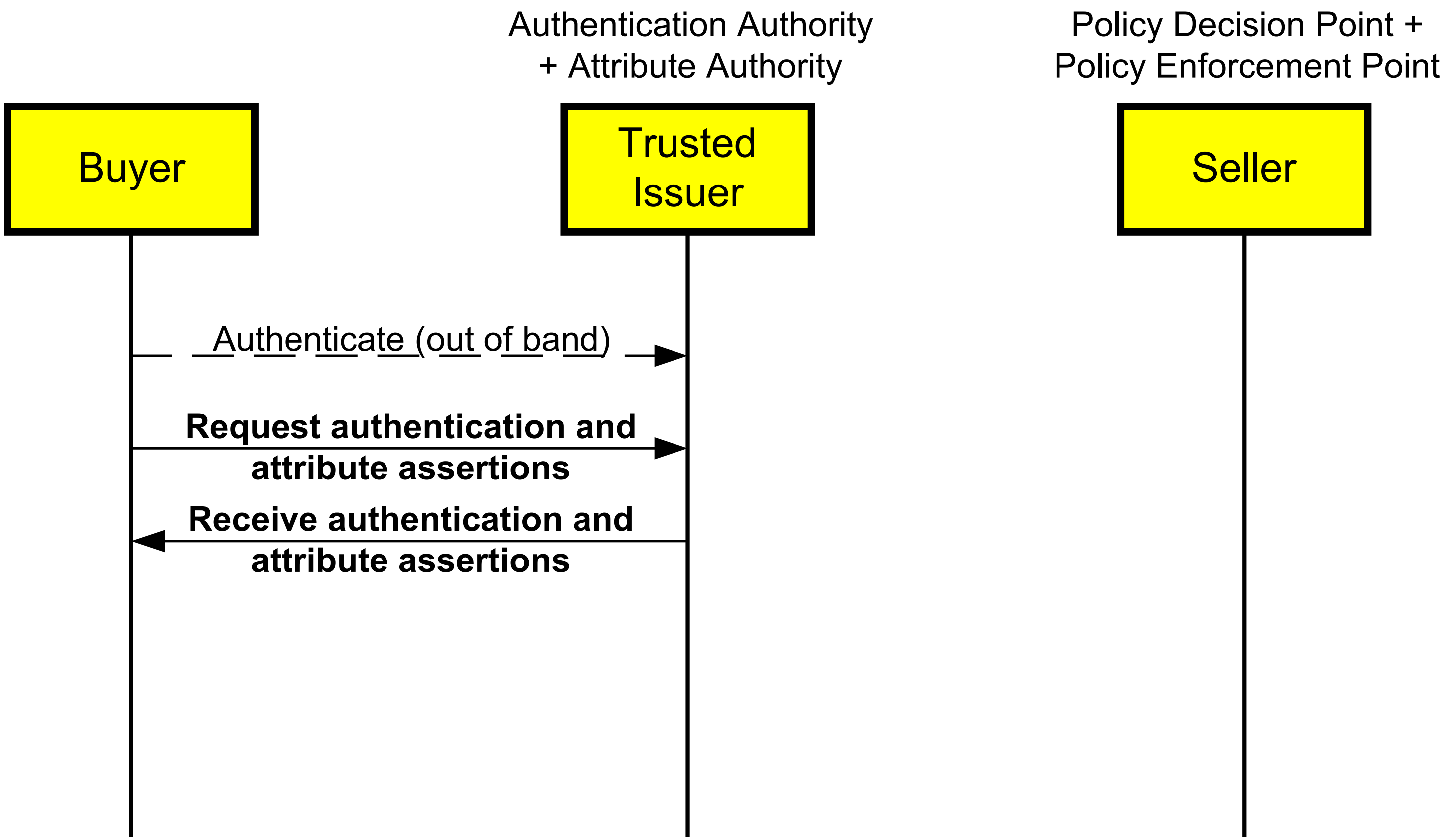


Authentication Authority + Attribute Authority

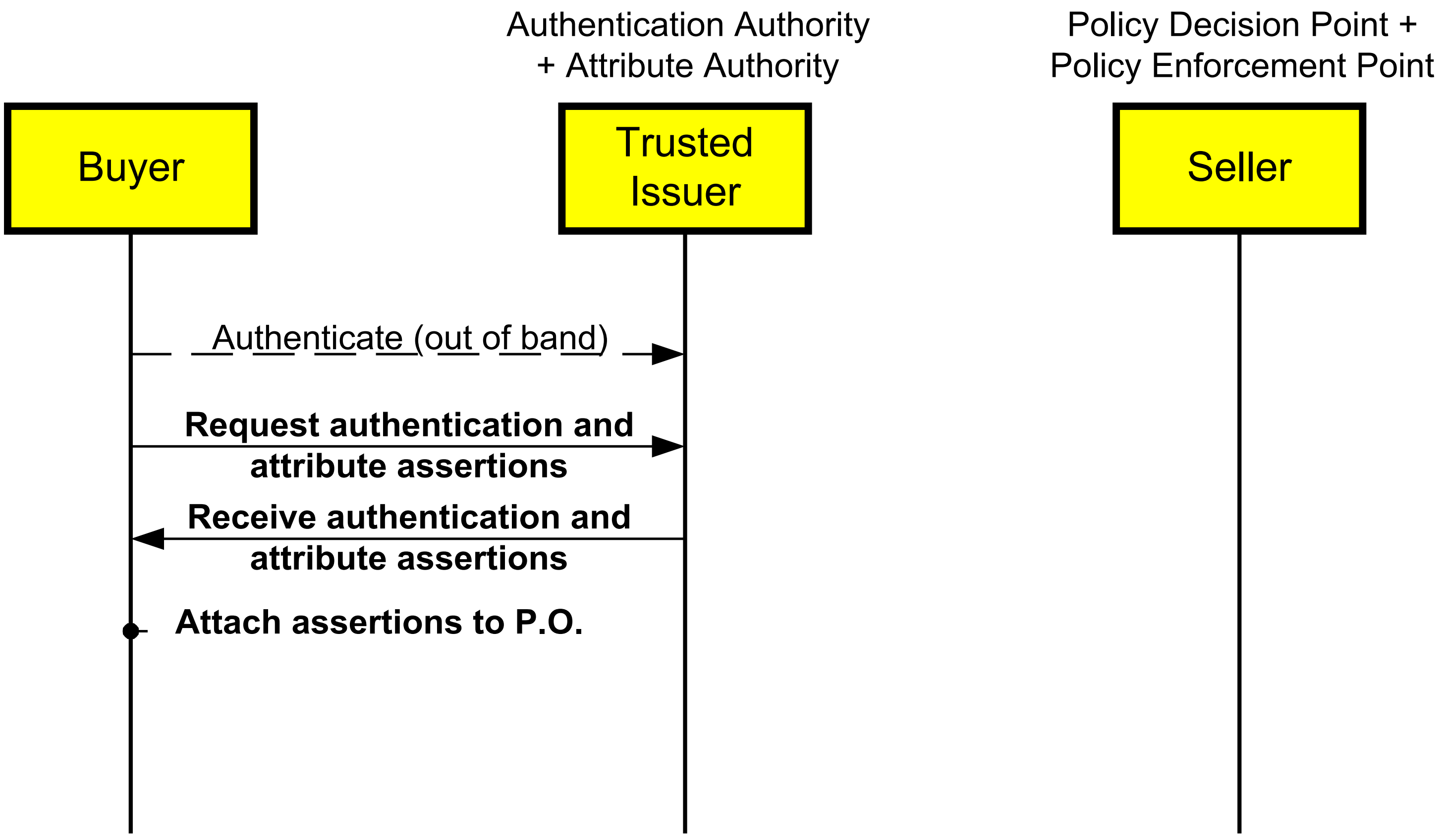
Policy Decision Point + Policy Enforcement Point

Buyer
Trusted Issuer
Seller
Authenticate (out of band)
Request authentication and attribute assertions

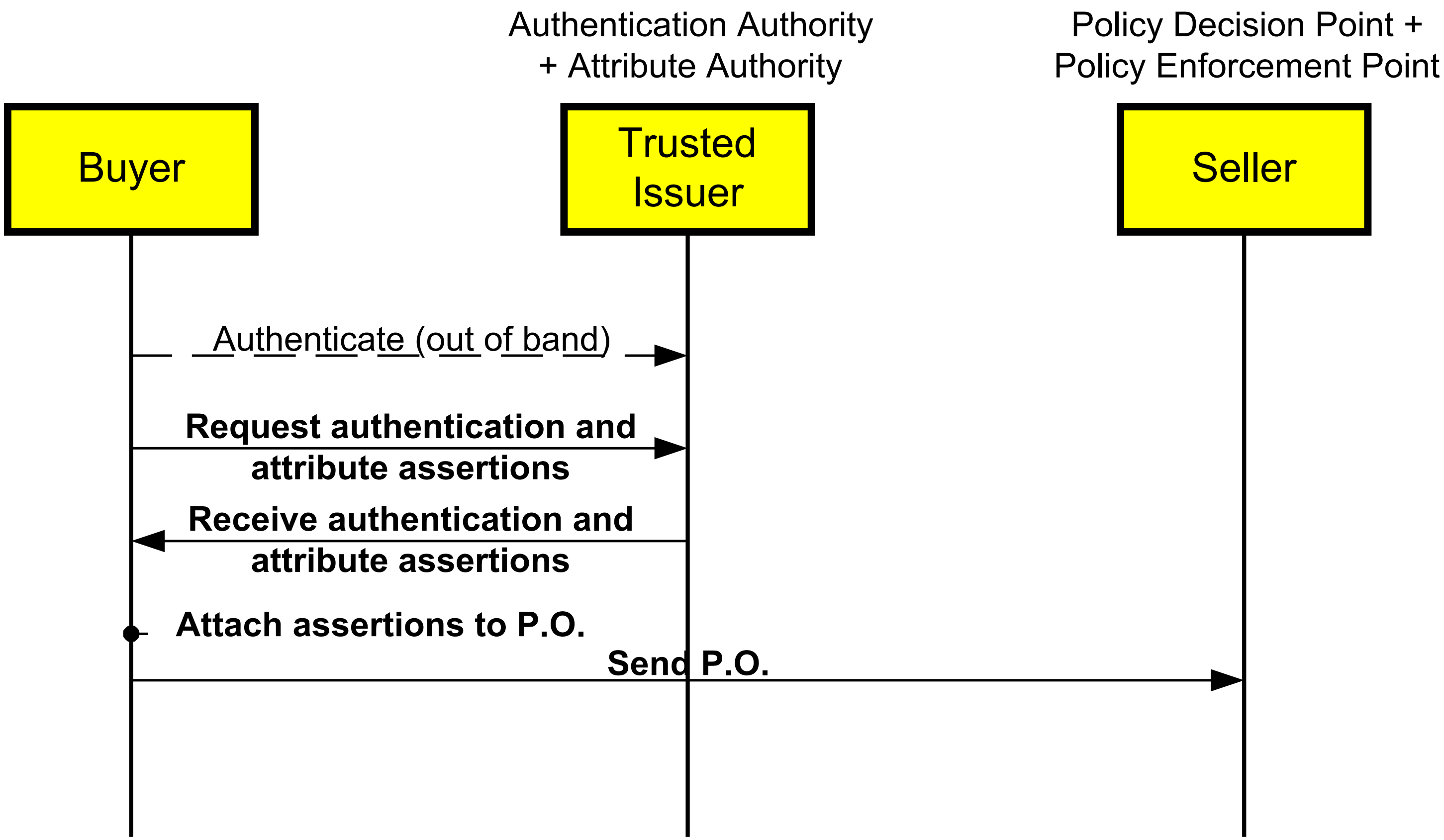
Distributed transaction scenario


Authentication Authority
+ Attribute Authority
Policy Decision Point +
Policy Enforcement Point
Buyer
Trusted Issuer
Seller
Authenticate (out of band)
Request authentication and attribute assertions
Receive authentication and attribute assertions

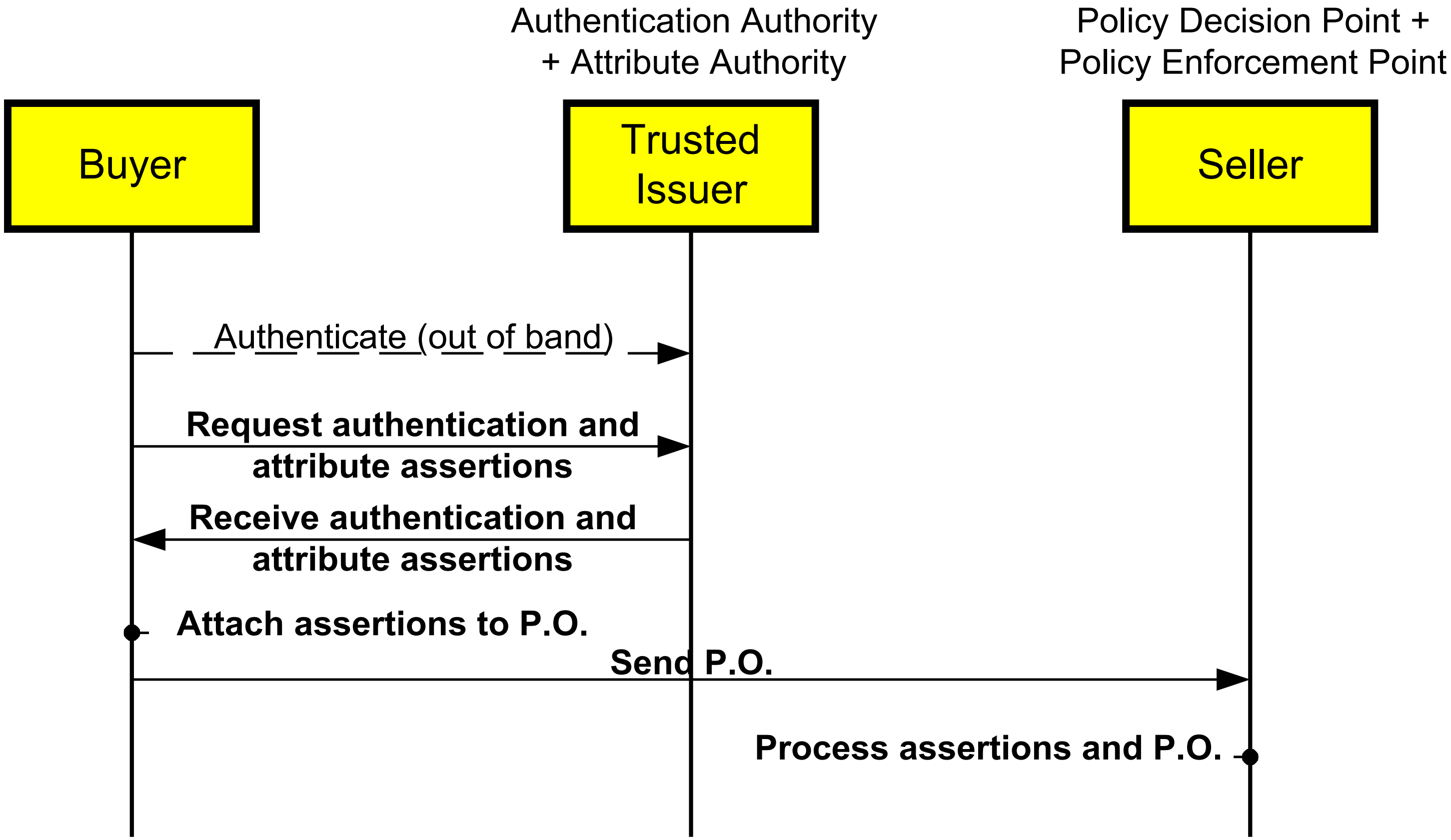
Distributed transaction scenario


Authentication Authority + Attribute Authority
Policy Decision Point + Policy Enforcement Point
Buyer
Trusted Issuer
Seller
Authenticate (out of band)
Request authentication and attribute assertions
Receive authentication and attribute assertions
Attach assertions to P.O.

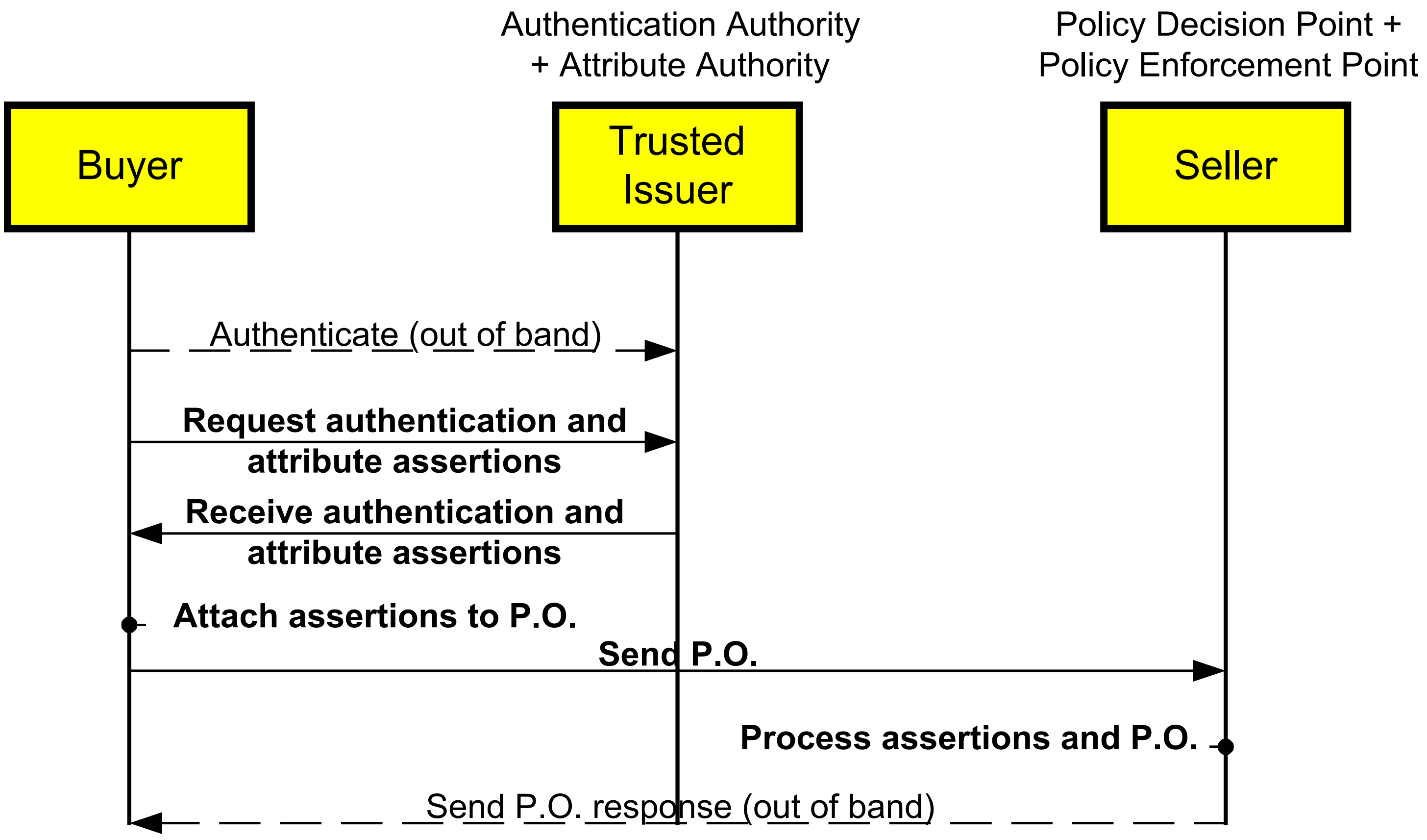
Distributed transaction scenario


Authentication Authority
+ Attribute Authority
Policy Decision Point +
Policy Enforcement Point
Buyer
Trusted Issuer
Seller
Authenticate (out of band)
Request authentication and attribute assertions
Receive authentication and attribute assertions
Attach assertions to P.O.
Send P.O.

Distributed transaction scenario


Authentication Authority
+ Attribute Authority
Policy Decision Point +
Policy Enforcement Point
Buyer
Trusted Issuer
Seller
Authenticate (out of band)
Request authentication and attribute assertions
Receive authentication and attribute assertions
Attach assertions to P.O.
Send P.O.
Process assertions and P.O.

Distributed transaction scenario


Authentication Authority
+ Attribute Authority
Policy Decision Point +
Policy Enforcement Point
Buyer
Trusted Issuer
Seller
Authenticate (out of band)
Request authentication and attribute assertions
Receive authentication and attribute assertions
Attach assertions to P.O.
Send P.O.
Process assertions and P.O.
Send P.O. response (out of band)

More on the distributed transaction scenario

- An example of attaching SAML assertions to other traffic
- Asymmetrical relationship is assumed
  - Seller is already known to buyer, but buyer is not known to seller, a common situation
  - E.g., server-side certificates might be used to authenticate seller
- If it were symmetrical, additional SAML steps would happen on the right side too
  - This would likely be a different scenario

Agenda

- The problem space
- SAML concepts
- Walking through scenarios
- Status of SAML and helpful resources

SAML status

- A suite of five Committee Specs was published 19 April 2002 after 1¼ years of work
  - Core (with assertion and protocol schemas)
  - Bindings and profiles
  - Conformance
  - Glossary
  - Security considerations
- The SOAP profile is on a later track
  - We will be looking at WS-security and similar inputs
- Burton Catalyst conference will host SAML Interop 2002 in July with 13 vendors taking part
- SAML vote will be held June-October to achieve OASIS Standard status

SAML resources

- OASIS SAML Technical Committee
  - TC site: www.oasis-open.org/committees/security/
  - Archives: lists.oasis-open.org/archives/security-services/
- SAML developers' mailing list
  - Archives: lists.oasis-open.org/archives/saml-dev/
  - Subscribe: lists.oasis-open.org/ob/adm.pl
- XML Cover Pages SAML page
  - xml.coverpages.org/saml.html
- Netegrity SAML information and JSAML toolkit
  - www.netegrity.com/products/

Some resources for related efforts

- IETF/W3C XML Signature
  - www.w3.org/Signature/
- W3C XML Encryption
  - www.w3.org/Encryption/2001/
- XKMS and its relatives (now at W3C)
  - www.w3.org/TR/xkms/
- OASIS XACML
  - www.oasis-open.org/committees/xacml/
- OASIS Provisioning
  - www.oasis-open.org/committees/provision/
- Liberty Alliance
  - www.projectliberty.org
- Internet2
  - www.internet2.edu/

Agenda

- The problem space
- SAML concepts
- Walking through scenarios
- Status of SAML and helpful resources
- Questions?

Thank you

Eve Maler
eve.maler@sun.com