SAML 2.0 and Related Work in XACML and WS-Security

Hal Lockhart

BEA Systems

Acknowledgements

- Many of the slides provided by
  - Eve Maler, Sun Microsystems
  - Prateek Mishra, Principal Identity
  - Rob Philpott, RSA Security

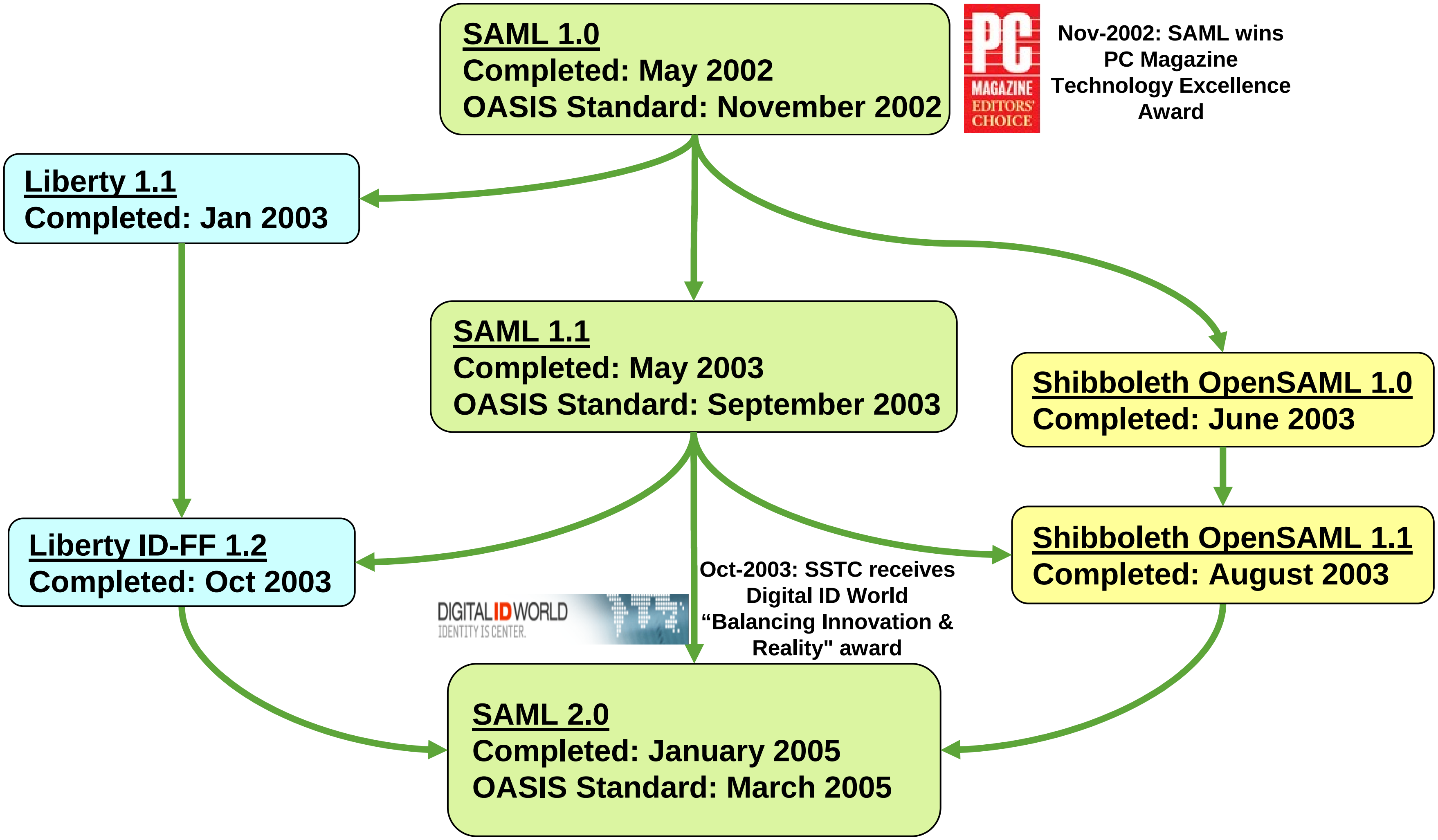
Agenda

- SAML History and Overview
- SAML 2.0 New Features
- SAML-related features in XACML
- SAML in Web Services Security

SAML and the OASIS SSTC

- SAML: Security Assertion Markup Language
  - A framework for the exchange of security-related information between trusting parties
  - The key standard for federated identity systems
  - Supports many real-world business scenarios
  - Widely used today for cross-domain single sign-on
- OASIS Security Services Technical Committee (SSTC)
  - SSTC manages SAML development
  - 36 current voting members representing 24 organizations

SAML Timeline



SAML 1.0
Completed: May 2002
OASIS Standard: November 2002

Nov-2002: SAML wins
PC Magazine
Technology Excellence
Award

Liberty 1.1
Completed: Jan 2003

SAML 1.1
Completed: May 2003
OASIS Standard: September 2003

Shibboleth OpenSAML 1.0
Completed: June 2003

Liberty ID-FF 1.2
Completed: Oct 2003

Shibboleth OpenSAML 1.1
Completed: August 2003

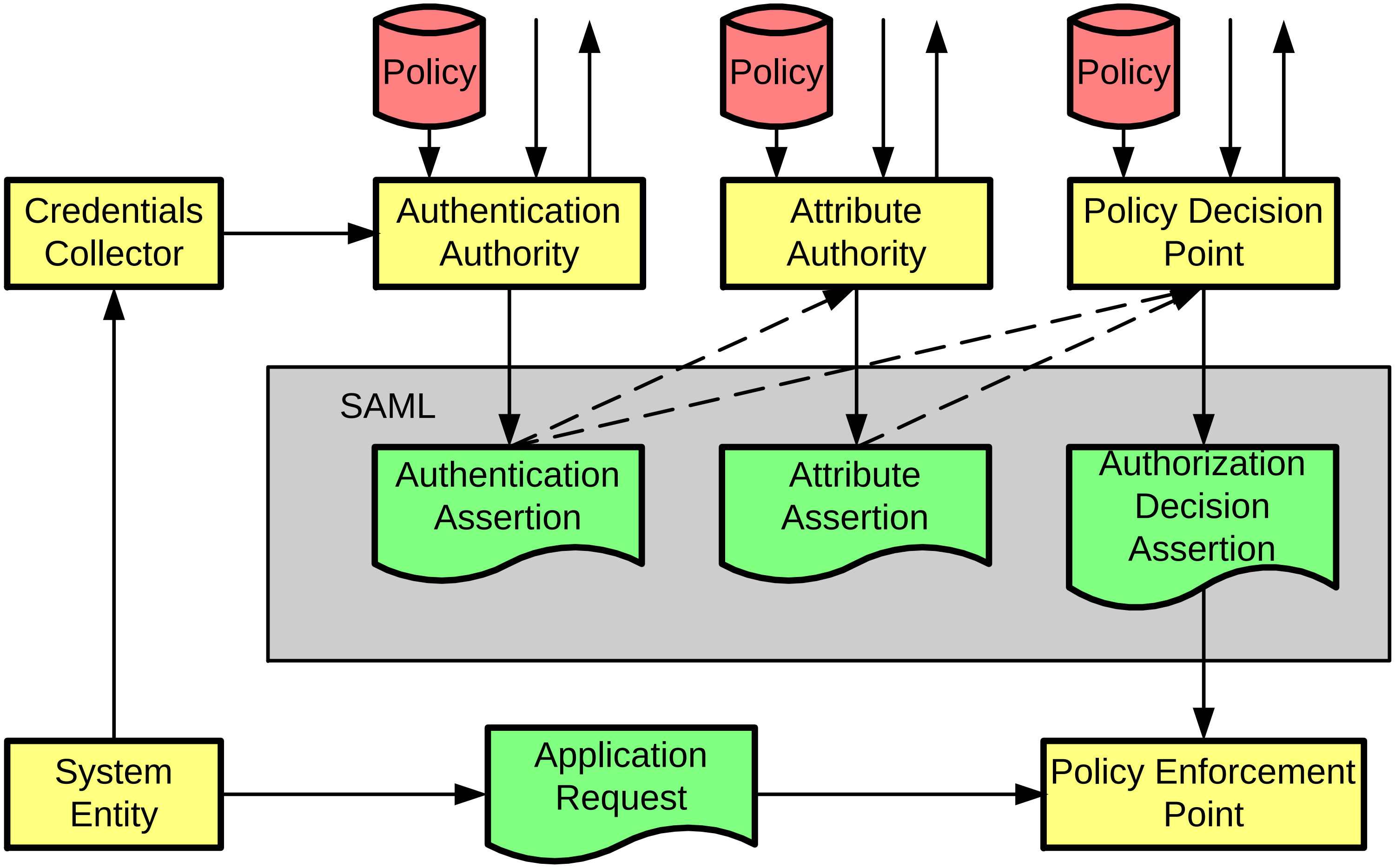
Oct-2003: SSTC receives
Digital ID World
“Balancing Innovation &
Reality" award

SAML 2.0
Completed: January 2005
OASIS Standard: March 2005

Specification Suite

- Conformance Requirements
  - Required “Operational Modes” for SAML implementations
- Assertions and Protocols
  - The “Core” specification
- Bindings
  - Maps SAML messages onto common communications protocols
- Profiles
  - “How-to’s” for using SAML to solve specific business problems
- Metadata
  - Configuration data for establishing agreements between SAML entities
- Authentication Context
  - Detailed descriptions of user authentication mechanisms
- Security and Privacy Considerations
  - Security and privacy analysis of SAML 2.0
- Glossary
  - Terms used in SAML 2.0

SAML producer-consumer model



SAML assertions

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

All statements in an assertion share common information

- Issuer ID and issuance timestamp
- Assertion ID
- Subject
  - Name plus the security domain
  - Optional subject confirmation, e.g. public key
- "Conditions" under which assertion is valid
  - SAML clients *must reject* assertions containing unsupported conditions
  - Special kind of condition: assertion validity period
- Additional "advice"
  - E.g., to explain how the assertion was made

Authentication statement

- An issuing authority asserts that subject S was authenticated by means M at
  time T
- Targeted towards SSO uses

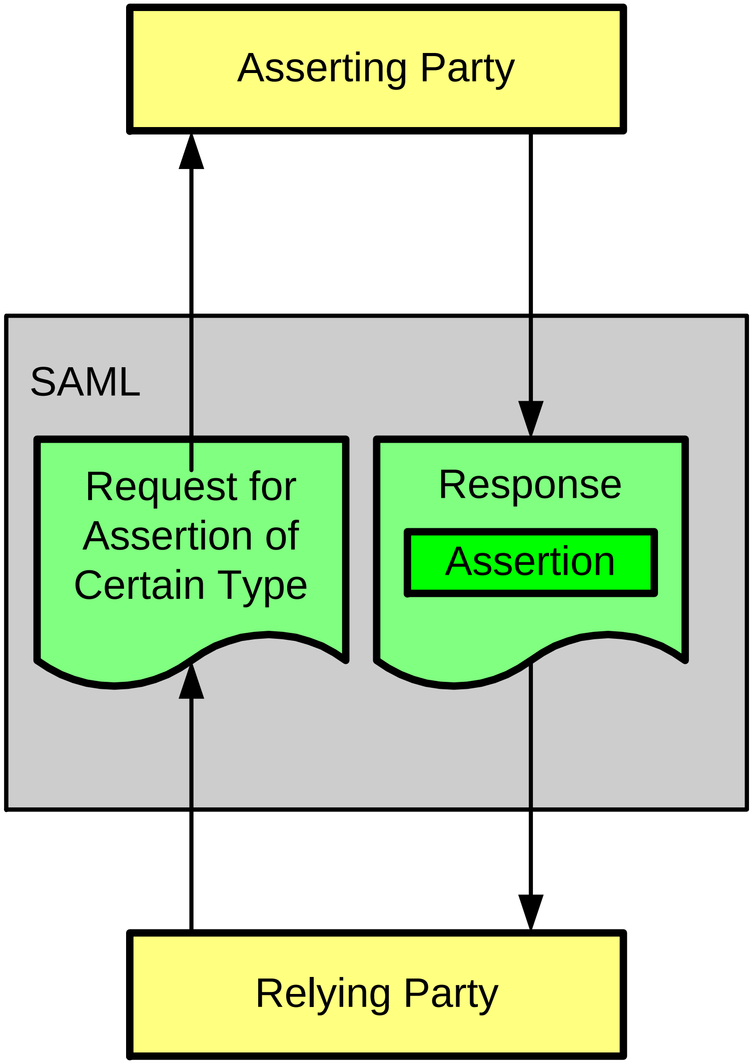
Attribute statement

- 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”

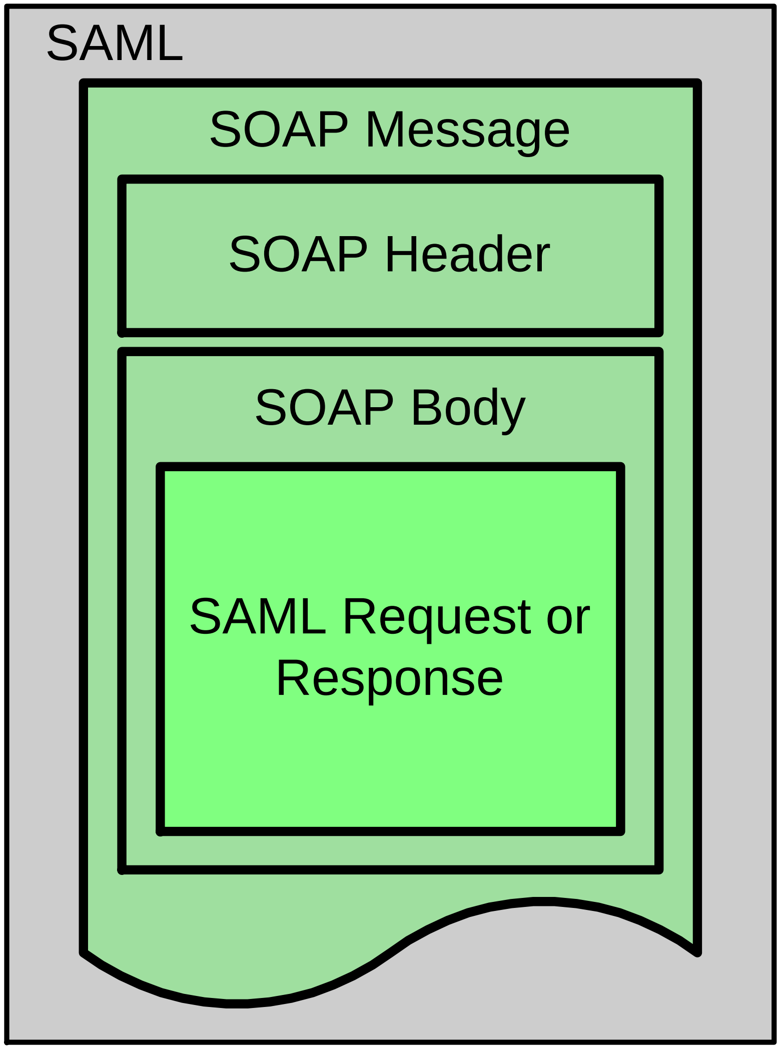
Authorization decision statement

- 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

SAML protocol for getting assertions



The SOAP-over-HTTP binding



Agenda

- SAML History and Overview
- SAML 2.0 New Features
- SAML-related features in XACML
- SAML in Web Services Security

SSTC SAML 2.0 Goals

- Continue SSTC tradition of focusing on real-world business problems
- SAML 2.0 Charter
  - Address issues and enhancement requests that have arisen from experience with real-world SAML implementations and with other security architectures that use SAML.
  - Add support for features that were deferred from previous versions of SAML.
  - Develop an approach for unifying various identity federation models found in real-world SAML implementations and SAML-based security architectures.

Business Benefits

- Platform and vendor neutrality
- Support for new devices
- Consistent online user experience
- Unified approach to identity federation
- Improved control over identity data helps meet regulatory compliance requirements
- Privacy protection and user consent mechanisms
- Reduced deployment and administrative costs

SAML 2.0 New Features

- Robust identity federation and management
- Enhanced web single sign-on profile
- Identity provider discovery
- Basic session management and global logout
- Encrypted attributes, name identifiers, and assertions
- Profiles for well-defined attribute sharing
- Fine-grained description of authentication mechanisms
- Metadata for simplified configuration
- Enhanced Client or Proxy (ECP) profile

Identity Federation

- What is Identity Federation?
  - Agreement between providers concerning data used to identify users
    - User-specific attributes:
      - E-mail address?
      - Office number and Employee Id?
      - Role or membership in certain groups?
    - Unique, privacy-preserving identifiers known only to the providers?
  - Federated identifiers can be created in different ways
    - Dynamic assignment based on business agreements
    - Dynamic creation based on user consent
    - Out-of-band bulk synchronization or update at both parties

Identity Federation and Mgmt

- Multiple types of Name Identifiers
  - Well-known names
    - Email Address
    - X.509 Subject Name
    - Windows Domain Qualified Name
    - Kerberos Principal Name
  - Privacy-preserving pseudonym identifiers
    - Transient
    - Persistent
  - Name Identifier Management Protocol and Profile
    - Assign new pseudonym identifiers
    - Terminate identity federation

Session Mgmt and Logout

- Session Participants
  - Identity Providers act as session authorities
  - Service Providers act as session participants
  - IdP defines session identifier(s) for SP’s
  - User may initiate logout at IdP or SP to terminate session
  - User may terminate individual or all active sessions
- Follows ID-FF 1.2 closely (logout but no timeout) but also provides extension points for richer session models
  - Instructions for privacy preservation are provided

Standard Attribute Profiles

- Supports attribute naming and values drawn from a variety of syntaxes
  - Basic Attribute Profile: string names and attribute values drawn from XML schema primitive types
  - X.500/LDAP Attribute Profile: use of canonical X.500/LDAP attribute names and values
  - UUID Attribute Profile: Use of UUIDs as attribute names
  - XACML Attribute Profile: formats suitable for processing by XACML
- Attribute statements may be transferred during SSO or by the use of the AttributeQuery protocol
- Attributes may be encrypted to ensure end-to-end confidentiality

Name Identifier Management

- Protocol for communicating information about name identifiers
  - When identifiers should be updated
    - Replace jsmith@foo.com by johns@foo.com
    - Rollover privacy preserving identifier at SP every 6 months
    - Update identifier at IdP with identifier meaningful to SP
  - When an identifier will no longer be acceptable for federation
    - IdP will not issue any more assertions for jsmith@foo.com
    - SP will not accept assertions for jsmith@foo.com

Metadata

- Improves deployment configuration of SAML components
- Identifies distinct roles supported by an entity
  - SSO Identity Provider
  - SSO Service Provider
  - Attribute Authority
  - Authentication Authority
  - Policy Decision Point
- Defines configuration and trust data such as:
  - Supported identifiers and profiles
  - SAML service endpoint URLs
  - Signing and encryption certificates
- Metadata Publication and Resolution

Agenda

- SAML History and Overview
- SAML 2.0 New Features
- SAML-related features in XACML
- SAML in Web Services Security

eXtensible Access Control Markup Language (XACML)

- Define a core XML schema for representing authorization and entitlement policies
- Target - any object - referenced using XML
- Fine grained control, characteristics - access requestor, protocol, classes of activities, and content introspection
- Consistent with and building upon SAML

XACML Objectives

- Ability to locate policies in distributed environment
- Ability to federate administration of policies about the same resource
- Base decisions on wide range of inputs
  - Multiple subjects, resource properties
- Decision expressions of unlimited complexity
- Ability to do policy-based delegation
- Usable in many different environments
  - Types of Resources, Subjects, Actions
  - Policy location and combination

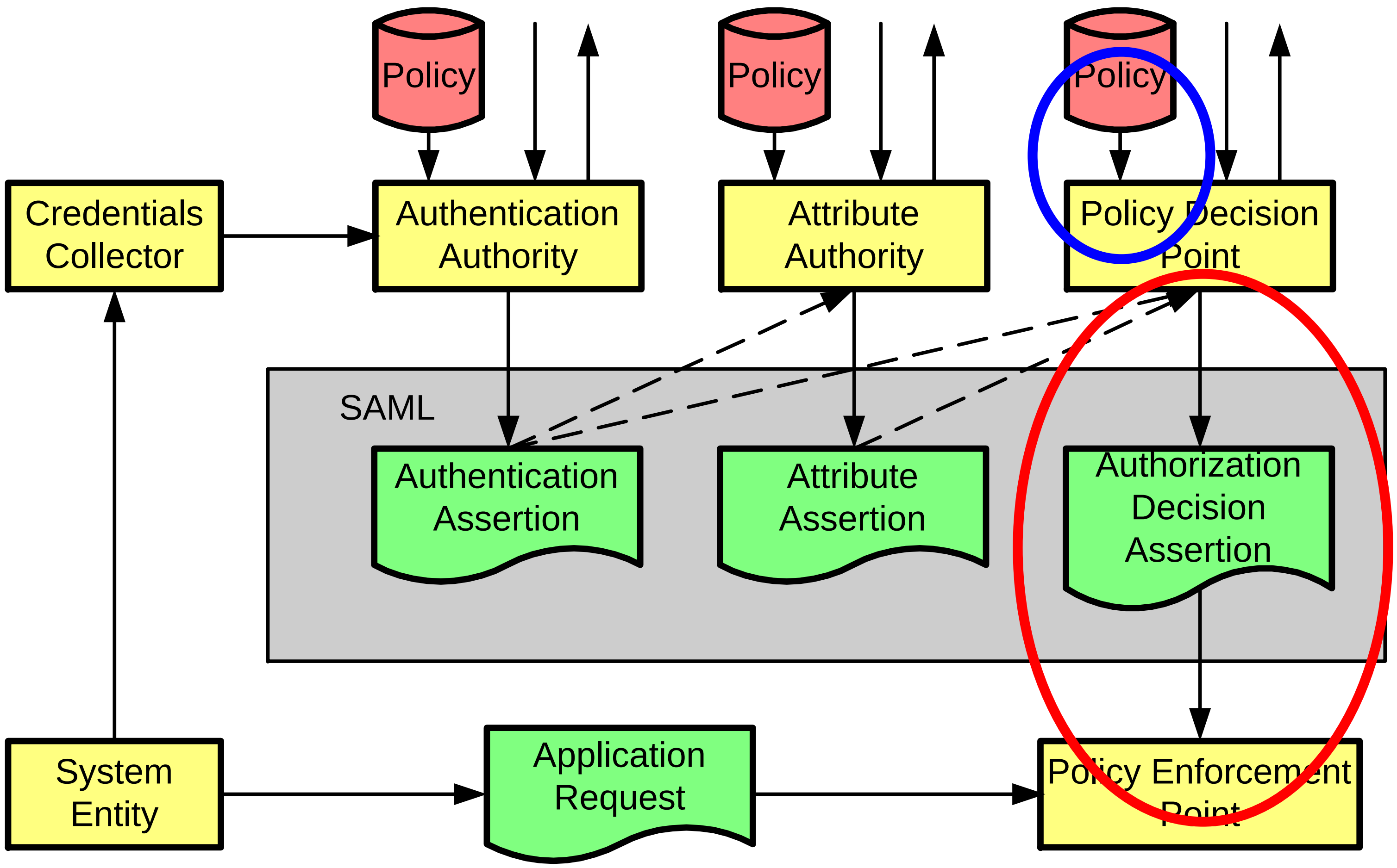
XACML History

- First Meeting – 21 May 2001
- Requirements from: Healthcare, DRM, Registry, Financial, Online Web, XML Docs, Fed Gov, Workflow, Java, Policy Analysis, WebDAV
- XACML 1.0 - OASIS Standard – 6 February 2003
- XACML 1.1 – Committee Specification – 7 August 2003
- XACML 2.0 – OASIS Standard – 1 February 2005

XACML 2.0 – SAML Features

- SAML Attribute mapping
- Authorization Decisions
  - Query
  - Response (Statement)
- Policy Management
  - Policy Statement
  - Policy request/response

XACML 2.0 Uses SAML Features



Agenda

- SAML History and Overview
- SAML 2.0 New Features
- SAML-related features in XACML
- SAML in Web Services Security

Web Services Security (WSS)

- Provides protection of SOAP messages
- SOAP header element <Security>
- Digital signatures and encryption
- Greater flexibility than SSL/TLS
- Supports multiple Security Token types
  - Username/password
  - Binary: X.509 and Kerberos
  - XML: SAML and REL

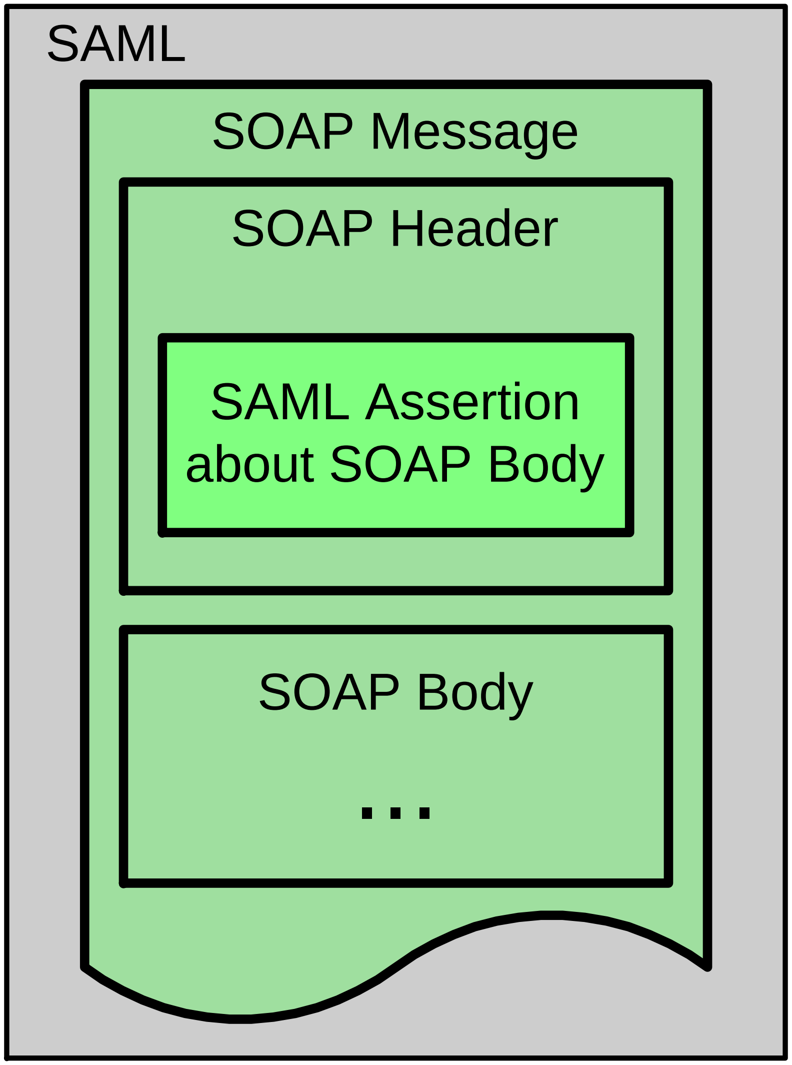
Web Services Security History

- OASIS TC formed September 2002
- OASIS Standard in April 2004
  - Core Specification + Username and X.509 Profiles
- OASIS Standard December 2004
  - SAML and REL Token Profiles
- Attachments Profile completed public review
- Kerberos Token Profile in process
- WSS Version 1.1 in Progress
  - Complete document update
  - Backward compatible

SAML Token Profile

- SAML Assertions in Security Header
- Primary usage Attribute Statements
- Subject Confirmation – Holder of Key
  - Digital signature or encryption
- Subject Confirmation – Sender Vouches
  - Also supported

WSS SAML Token Profile



SAML 2.0 Summary

- Convergence point for SAML 1.x, Liberty ID-FF, and Shibboleth as an OASIS Standard
- New customer-driven features to:
  - Reduce deployment and administrative costs
  - Improve control over identity data to help meet regulatory compliance requirements
  - Enhance the web user online experience
  - Enhance privacy and user control over identity data
- Complete identity federation solution with no missing “last mile” pieces
- Complementary features in WS-Security and XACML