



# The Venn of Identity, Federation, and Secure Web Services

Technical perspectives on the  
order of evolving standards.

Gary Ellison



**JASIG**



*Sun*  
microsystems  
We make the net work.

## Overall Presentation Goal

This presentation describes the relationship of SOAP Message Security, SAML, and Federated Identity standards as they pertain to the enablement of secure web service endpoints

# Presenter's Qualifications

- Gary Ellison
  - Chief Security Architect NICP,
  - Security Spec. Lead Liberty Alliance Project
  - J2SE Security Architect (1999-2002)
  - Author “Inside Java 2 Platform Security 2<sup>nd</sup> Ed.”
    - ISBN: 0201787911



# Agenda

- Concepts
- Standards Landscape
- Web Application Security
  - SAML, Shibboleth, Liberty ID-FF
- Web services Security
  - OASIS Web Services Security
  - Liberty Web Services Framework
  - MS/IBM WS Roadmap



# The Venn of Identity, Federation, and Secure Web Services

Technical perspectives on the  
order of evolving standards.

Key  
Concepts



**JASIG**



*Sun*  
microsystems  
We make the net work.

# Key Concepts

*Simplified Sign-On (aka Single Sign-On) and Single Logout*

- Simplified Sign-On allows a user to sign-on once at an authority and to be seamlessly signed-on when navigating to another site within the authentication domain of the authority without the need to authenticate again.
- Single Logout provides synchronized session logout functionality across all sessions that were authenticated by a particular identity provider.

# Key Concepts

## *Federation*

- Federation is the act of constituting an authority out of a number of separate organizations so that each member retains the management of its internal affairs.
- Network Identity is the fusion of network security and authentication, user provisioning and customer management, single sign-on technologies, and Web services delivery.
- A federated identity architecture delivers the benefit of simplified sign-on to users by determining resource access decisions without requiring the user's personal information to be stored centrally.

# Pardon the brevity

- SSTC – OASIS Security Service Technical Committee
  - SAML – Security Assertion Markup Language
- WSSTC – OASIS Web Services Security TC
  - WSS – Web services Security Specification
- ID-FF – Identity Federation Framework
- ID-WSF – Identity Web Services Framework
- XACML – eXtensible Access Control Markup Language
- XKMS – XML Key Management Specification
- XrML – eXtensible Rights Markup Language



# The Venn of Identity, Federation, and Secure Web Services

Technical perspectives on the  
order of evolving standards.

Standards Landscape



**JASIG**

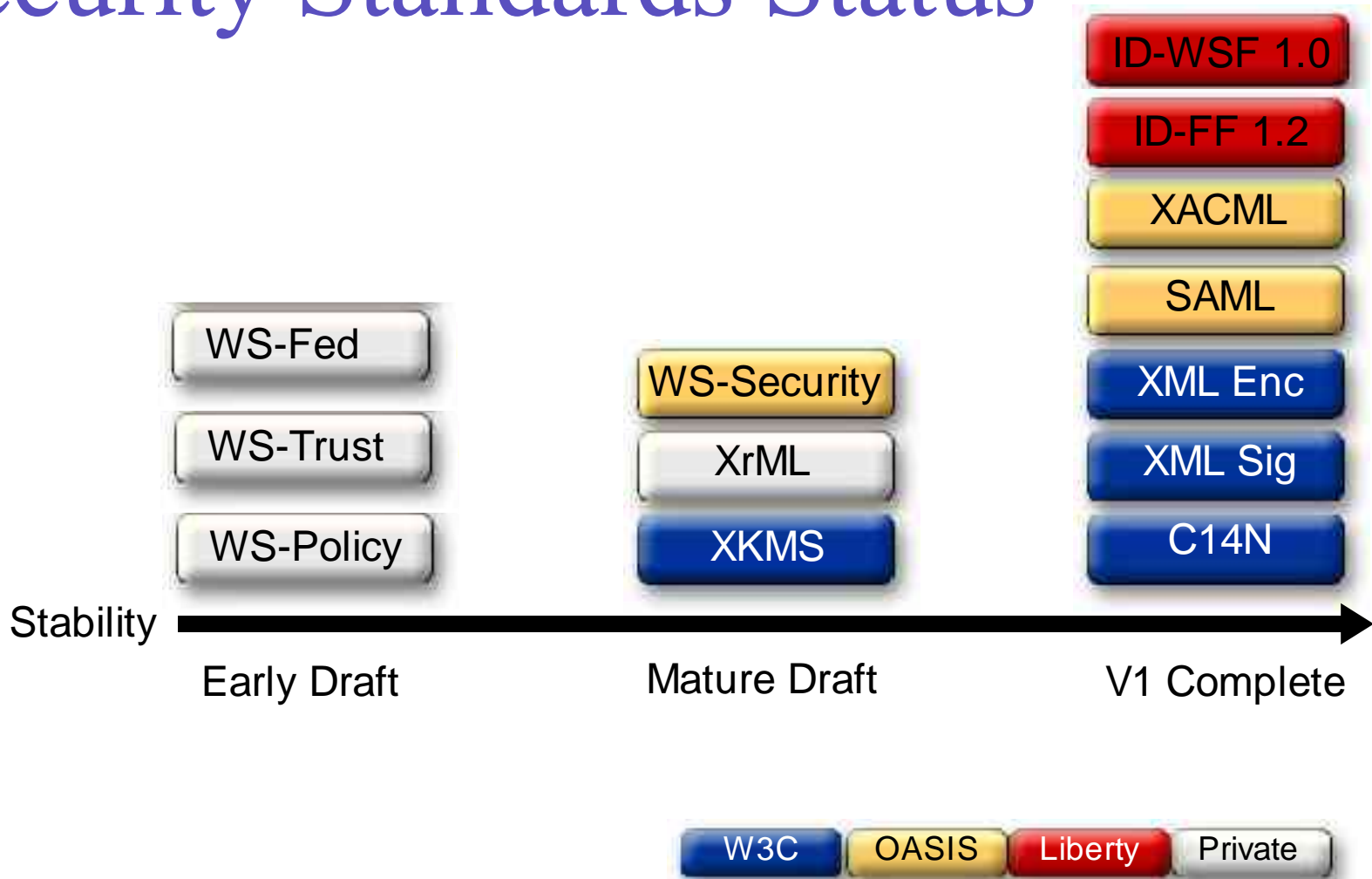


*Sun*  
microsystems  
We make the net work.

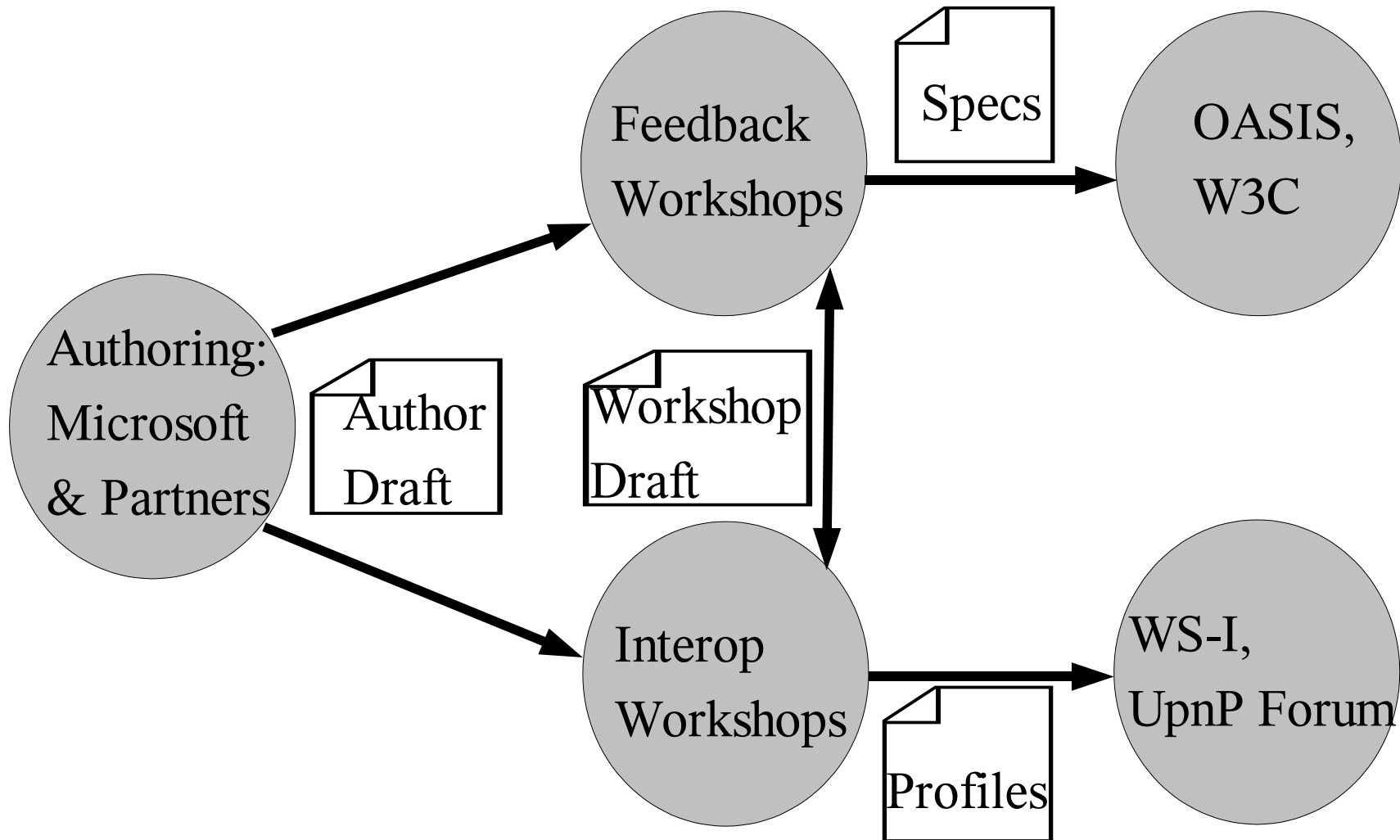
# Standards Status



# XML Web services Security Standards Status



# Microsoft Specification Development Process





# The Venn of Identity, Federation, and Secure Web Services

Technical perspectives on the  
order of evolving standards.

Web Application Security



**JASIG**



**Sun**  
microsystems  
We make the net work.

# Security Assertion Markup Language (SAML)

- XML-based framework for exchanging security assertions about:
  - Authentication
  - Attributes
  - Authorization decisions
  - Subjects (in general)
- Major usage scenarios so far:
  - Shibboleth uses SAML for SSO and Attributes Exchange
  - WS-Security profiles SAML for securing SOAP messages
  - Liberty uses SAML for Single Sign-On (SSO)
  - Liberty uses SAML to convey Identity to Web services

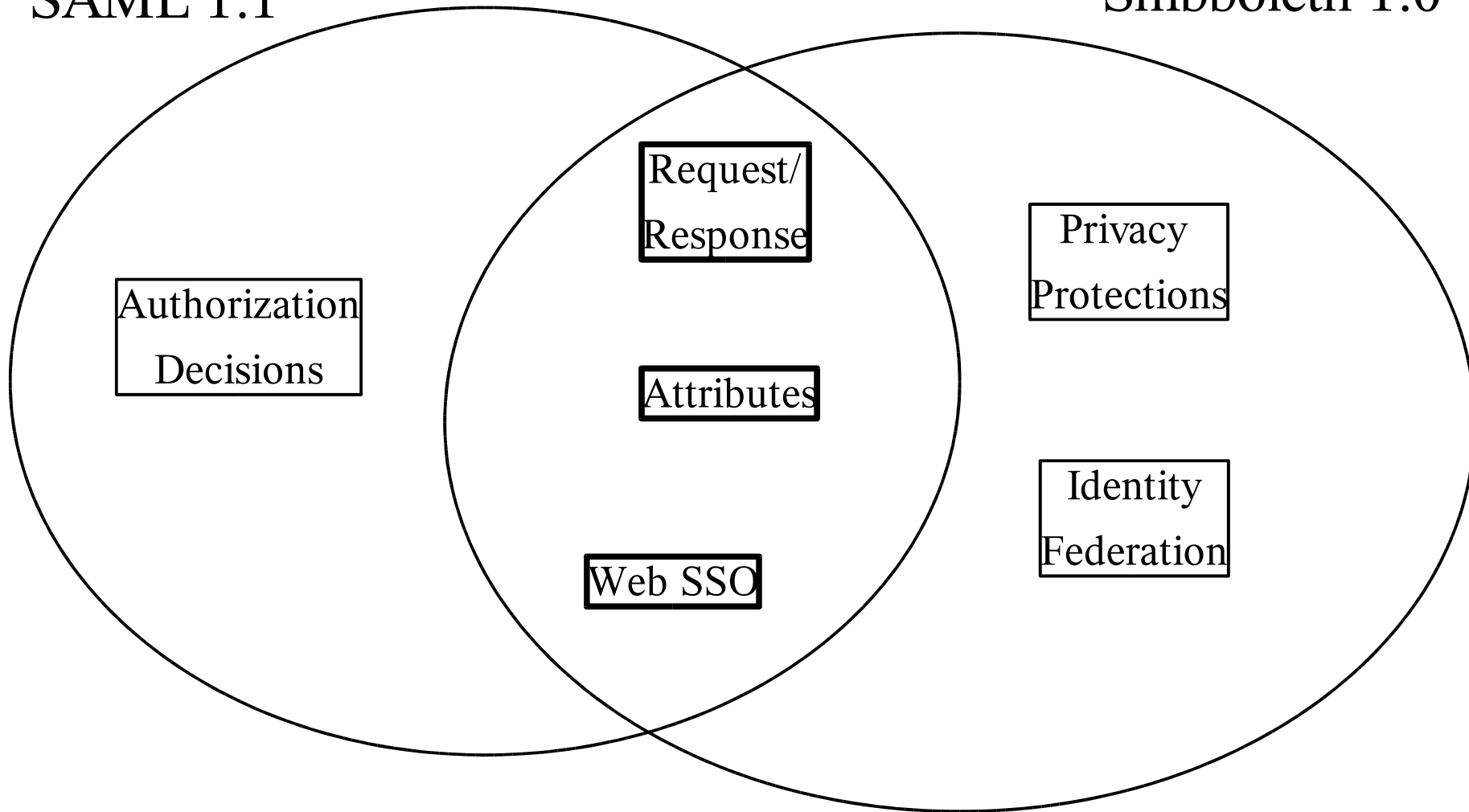
# Shibboleth SSO

- Uses SAML Browser/POST profile
- Attribute exchange use the SAML SOAP/HTTP binding
- Shibboleth Attribute Authorities are compliant SAML Attribute Authorities

# SAML $\cap$ Shibboleth Feature Use

SAML 1.1

Shibboleth 1.0



# Liberty Identity Federation Framework (ID-FF)

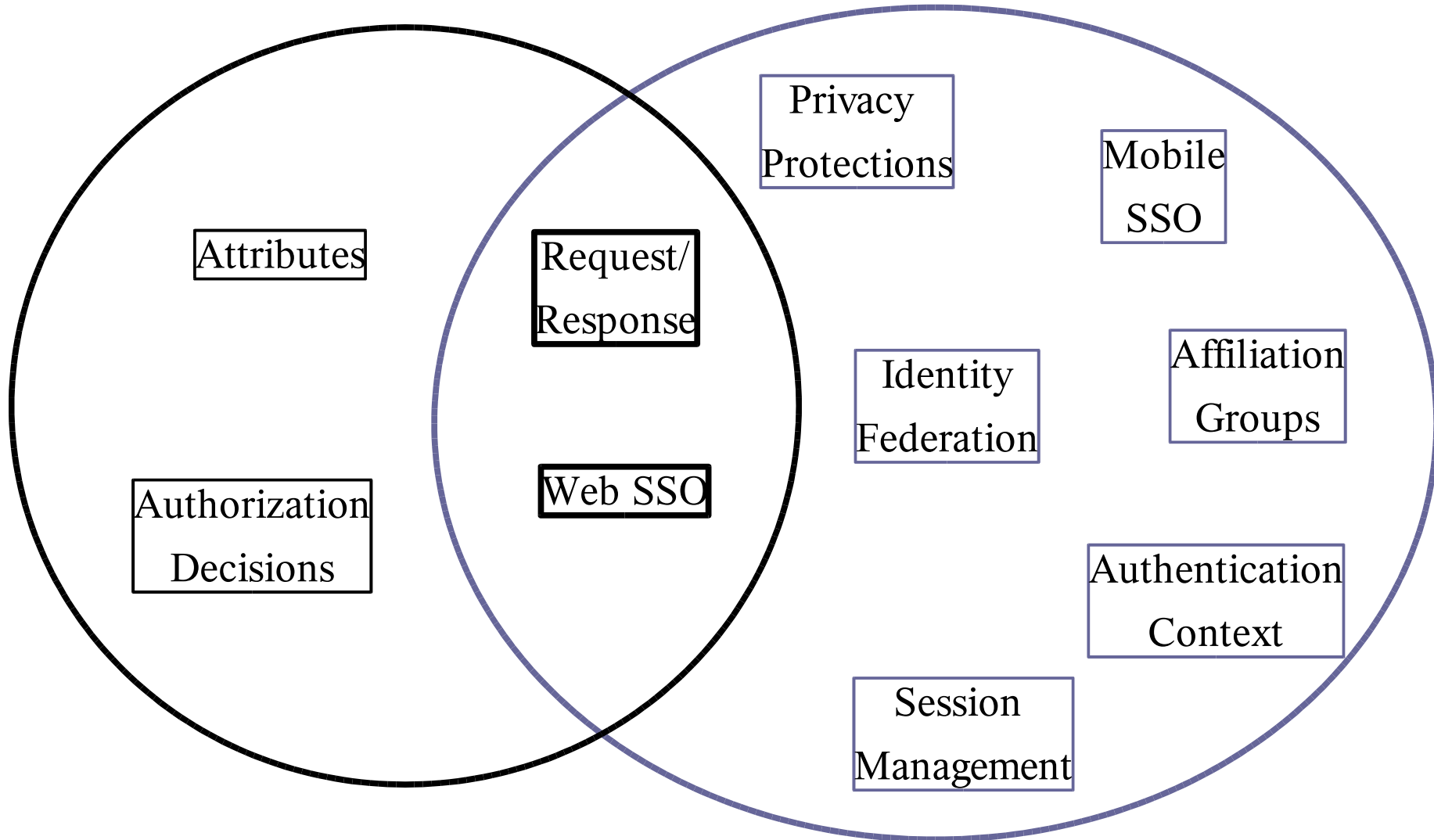


- **Protocols & Schemas:**
  - SSO, SLO
  - Federation, Federation Termination
  - Name Registration
- **Bindings and Profiles:**
  - 4 SSO/Federation profiles
  - 9 SLO profiles
- **Authentication Context**
- **Affiliations**
- **Metadata**
  - Defines provider communications policy
  - Exchange of metadata (endpoints, X.509 certs)

# SAML $\cap$ Liberty Feature Use

SAML 1.1

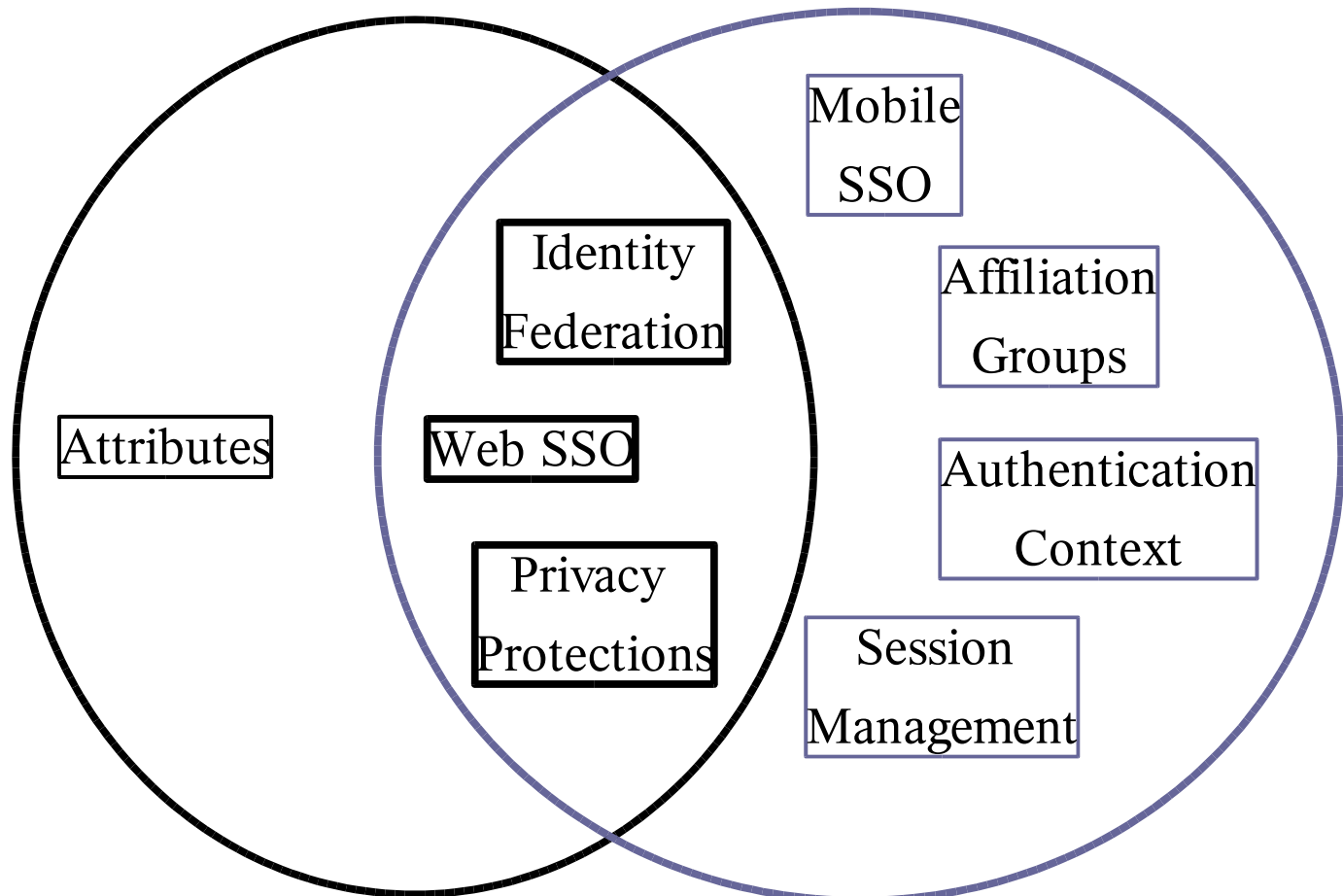
Liberty ID-FF 1.2



# Shibboleth $\cap$ Liberty Functions

Shibboleth 1.0

Liberty ID-FF 1.2





# The Venn of Identity, Federation, and Secure Web Services

Technical perspectives on the  
order of evolving standards.

Web services Security



**JASIG**



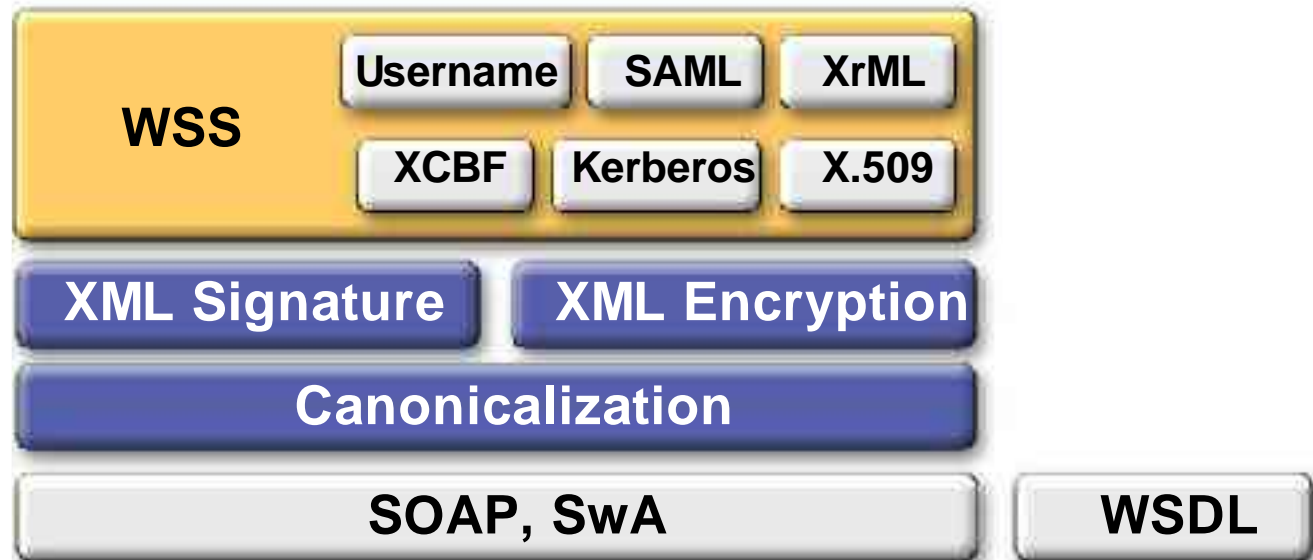
*Sun*  
microsystems  
We make the net work.

# Secure Web services Functional Areas

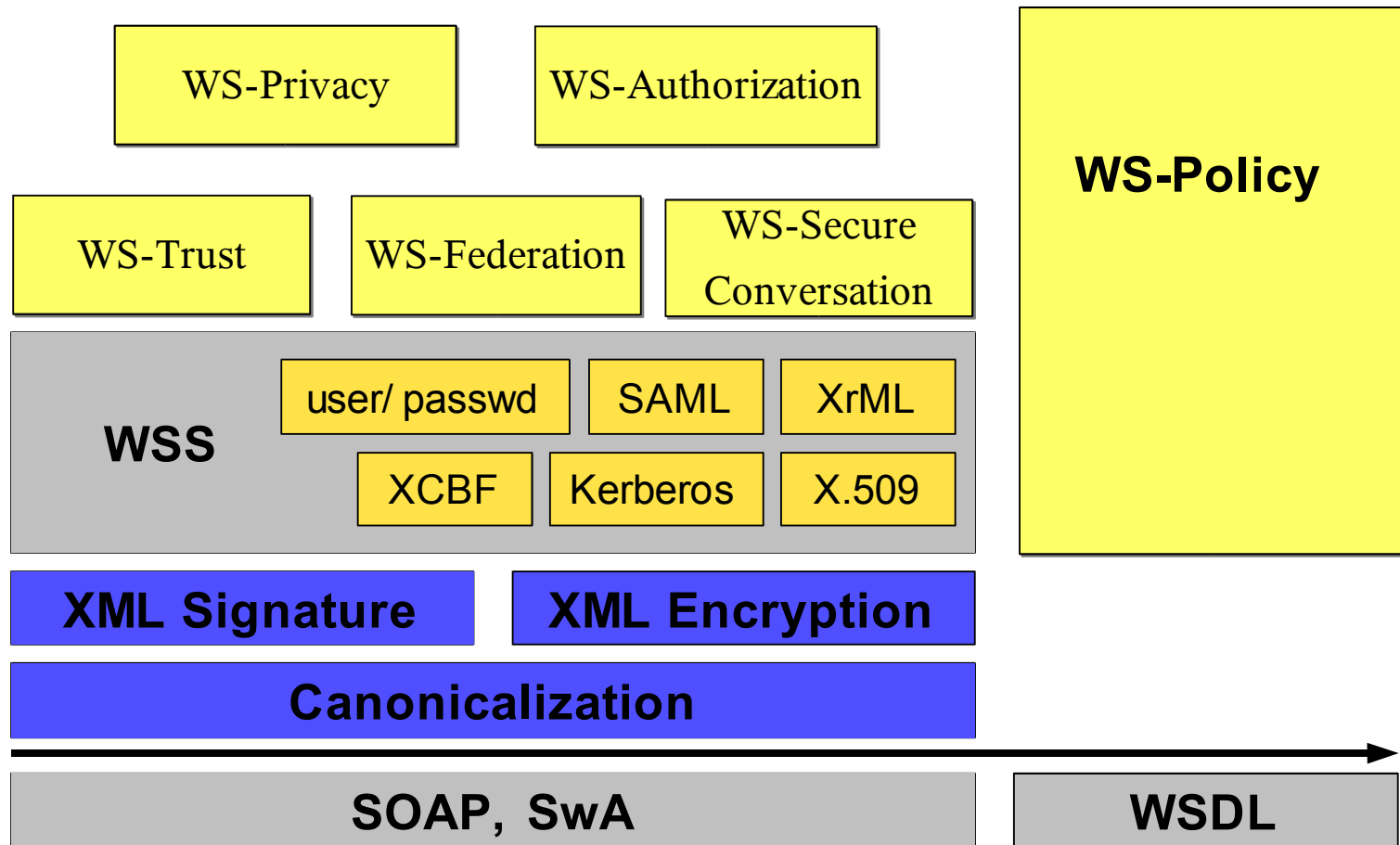


# Secure Web services Infrastructure Standards

**Authenticated, confidentiality-protected  
web service messages with potential  
to be authorized**



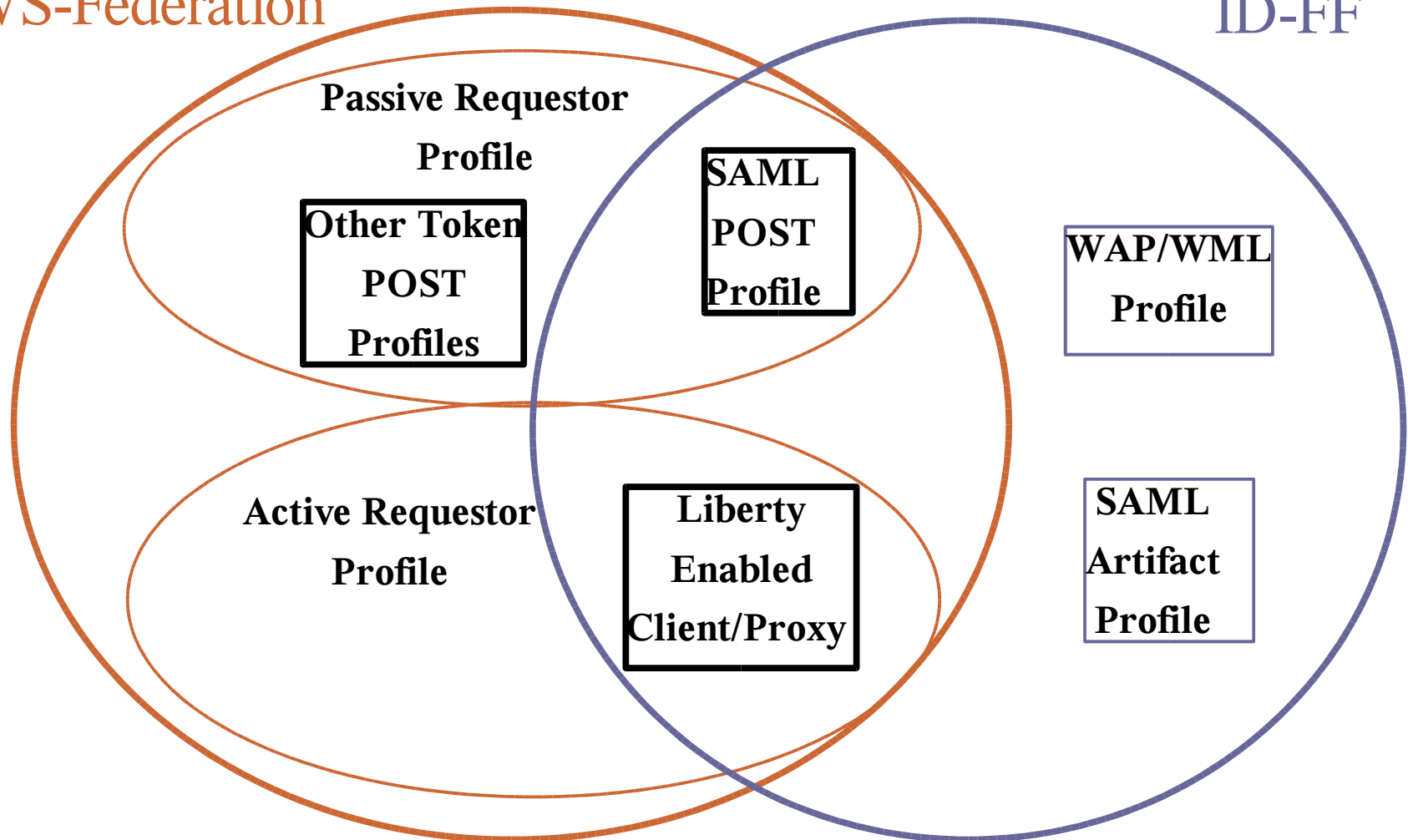
# MS/IBM Proposed Roadmap



# WS-Federation SSO $\cap$ ID-FF SSO

WS-Federation

ID-FF



# OASIS Web Services Security (WSS)

- Defines SOAP headers to provide:
  - Message integrity
  - Message confidentiality
  - Single-message authentication
- Associates a key via a “security token” with signed content
- Supports various security tokens:
  - Username/password
  - X.509 certificates
  - Kerberos tickets
  - SAML assertions
- Can carry data that supports authorization

# Liberty Identity Web Service Framework (ID-WSF)

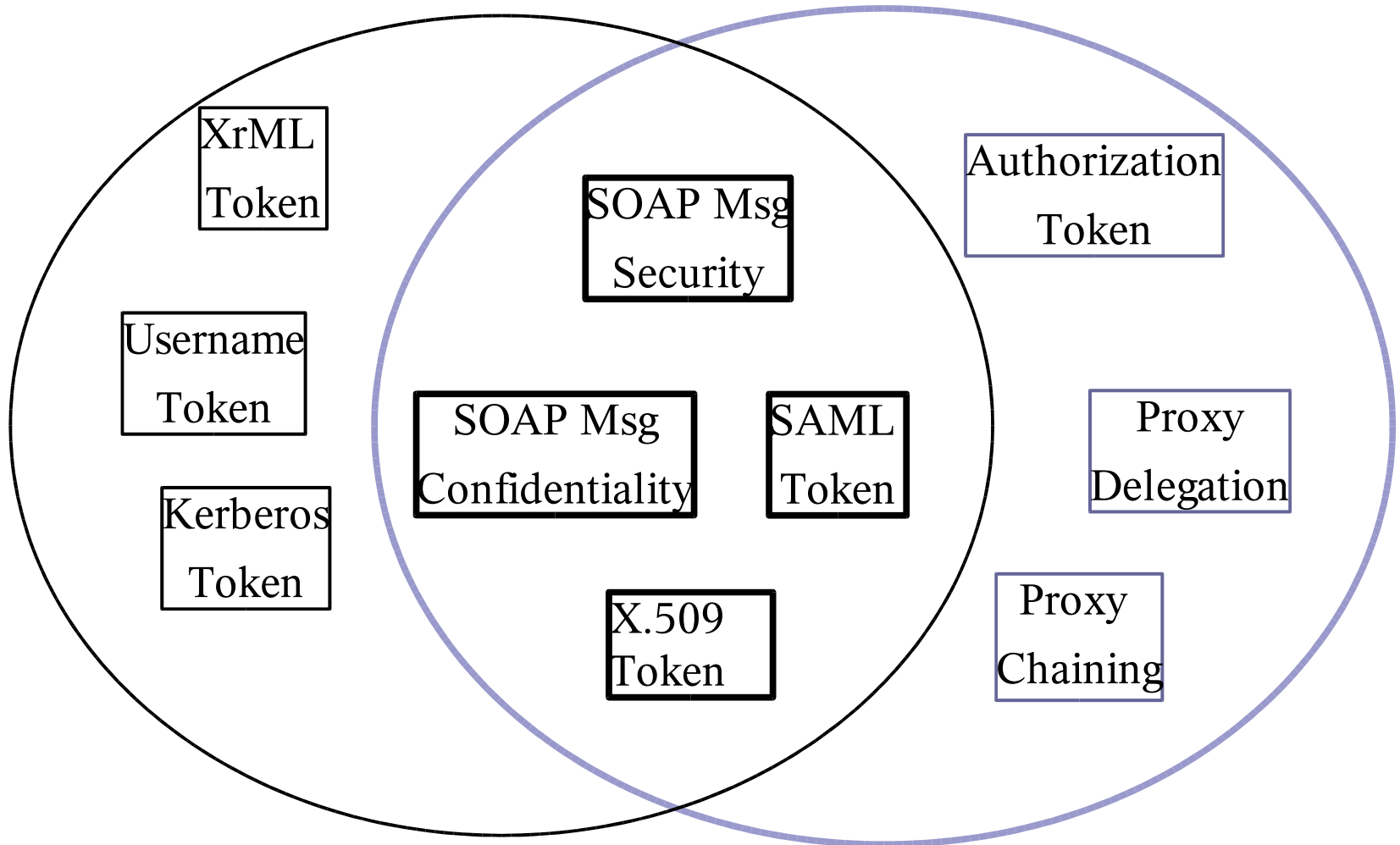
- Builds out “web service stack” to support and implement services useful to the Liberty members’ business models
- Examples include personal profile, mobile commerce, and location base services
- Leverages ID-FF for principal authentication, and federation, privacy protection, etc.
- Integrates service discovery and security token service

# ID-WSF Security Mechanisms

- Confidentiality and Privacy Protections
  - Transport Layer Channel Protection
  - Message Level Confidentiality Protection
  - Identifier Privacy Protection
- Peer Entity Authentication
  - Transport Layer Peer Authentication
- Message Level (Data Origin) Authentication
  - X.509 Certificate Based Mechanism
  - SAML Assertion Based Mechanism
- Message Level Authorization
  - Resource Access
  - Session Context

# WS-Security $\cap$ Liberty Feature Use

OASIS WS-Security drafts    Liberty ID-WSF Security Mech 1.0



# WS-Trust $\cap$ ID-WSF Functionality

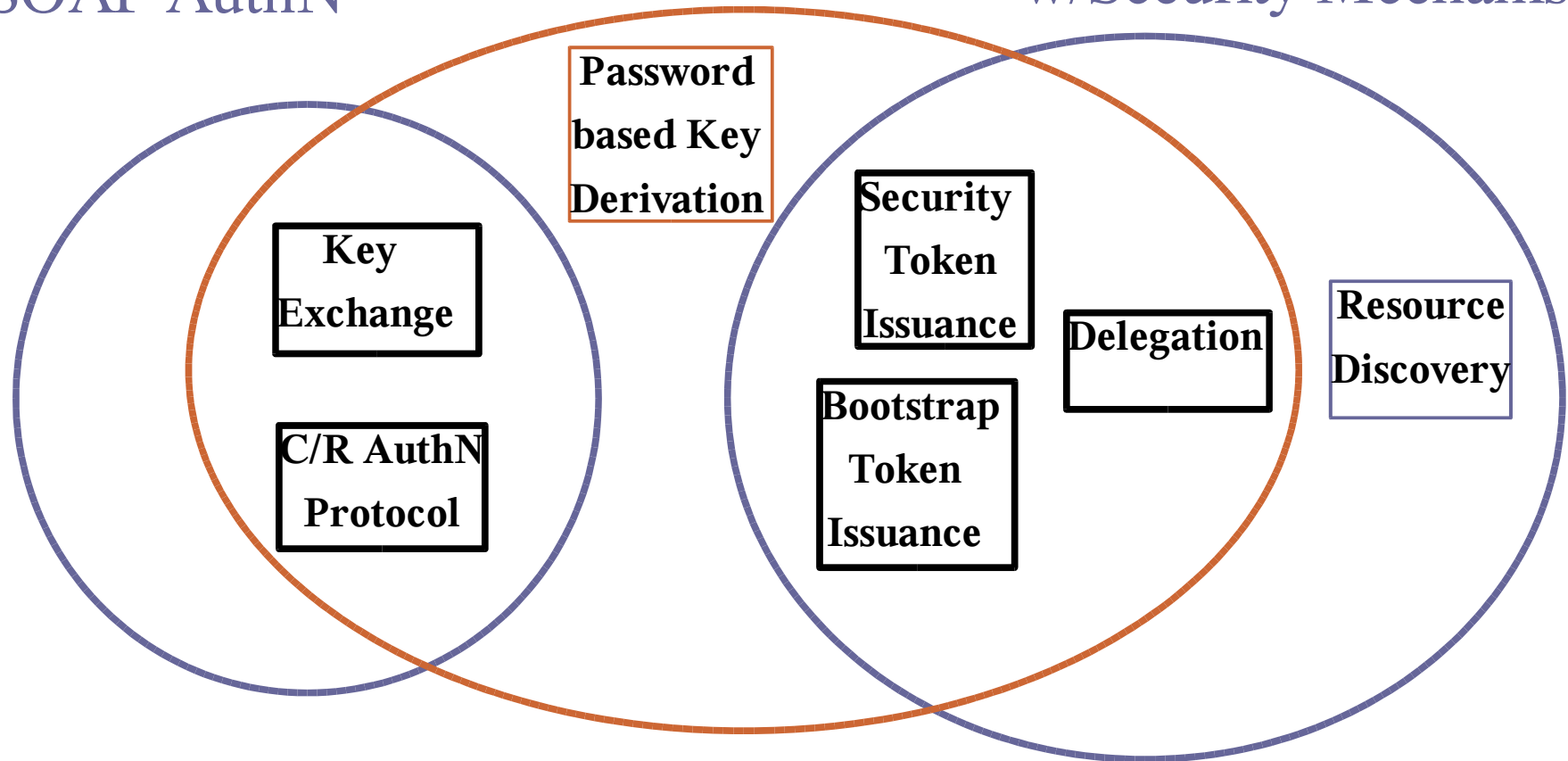
Liberty ID-WSF

WS-Trust

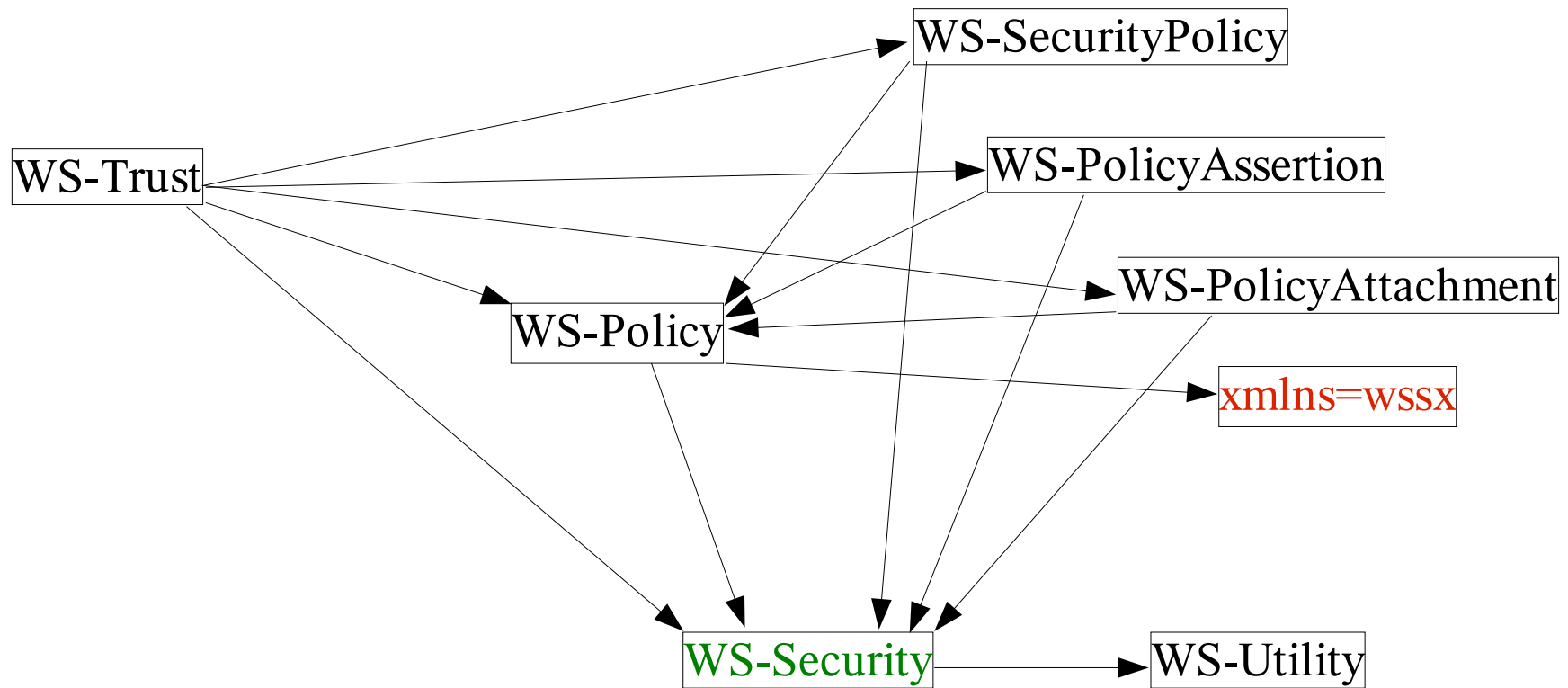
Liberty ID-WSF Discovery

SOAP AuthN

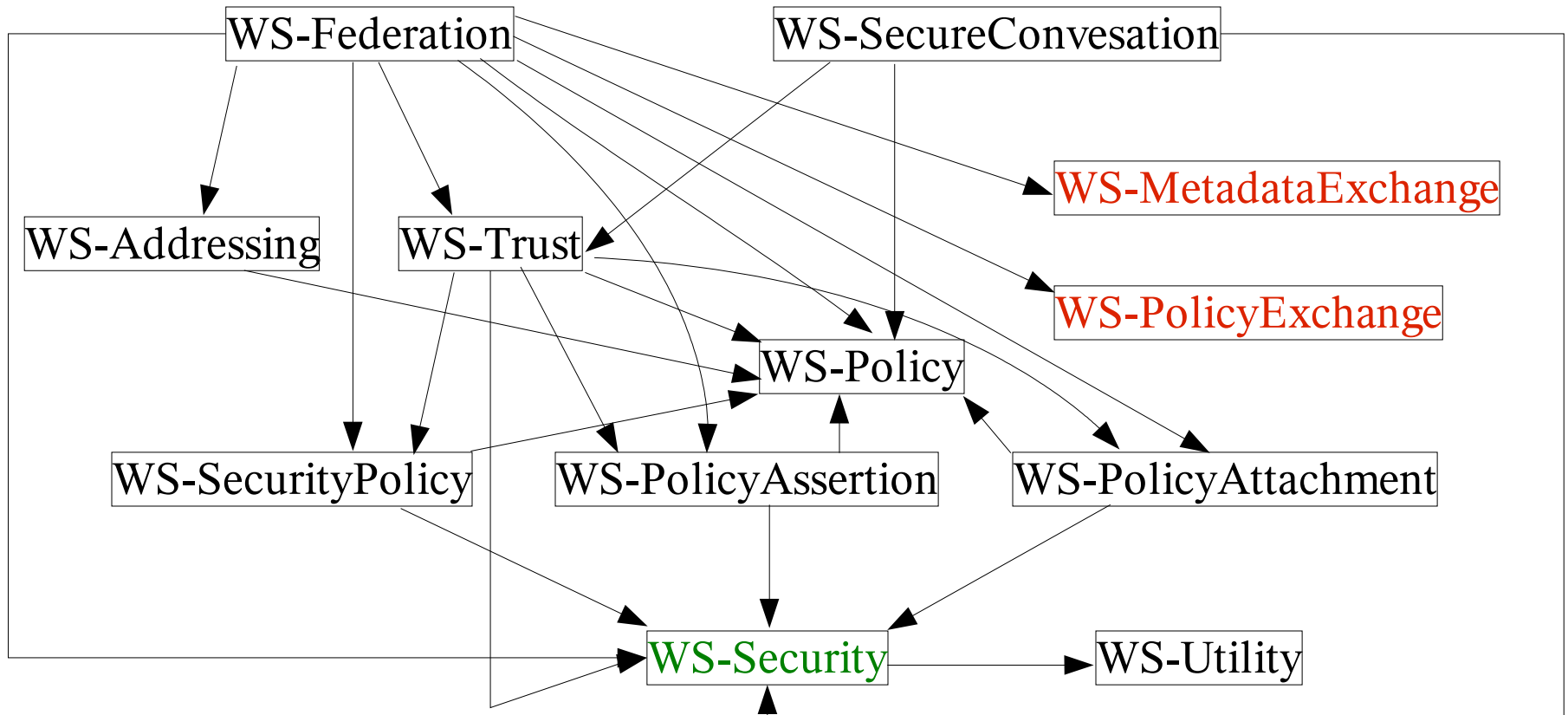
w/Security Mechanisms



# WS-Trust Depends



# WS-regex(5)





# Liberty enabled products & services

Communicator (available)  
Computer Associates (Q4\*)  
DataKey (available)  
DigiGan (Q3\*)  
Ericsson (Q4)  
Entrust (Q1 2004)  
France Telecom (Q4 2003)  
Fujitsu Invia (available)  
Gemplus (TBD)  
HP (available)  
July Systems (available)  
Netegrity (2004)  
NeuStar (available)  
Nokia (2004)  
Novell (available)

NTT (TBD)  
NTT Software (available)  
Oblivion (2004)  
PeopleSoft (available)  
Phaos Technology (available)  
Ping Identity (available)  
PostX (available)  
RSA (Q4)  
Salesforce.com (TBD)  
Sigaba (available)  
Sun Microsystems (available)  
Trustgenix (available)  
Ubisecure (available)  
Verisign (Q4\*)  
Vodafone (2004)  
WaveSet (available)

# Participation, Evaluation, Adoption

- Participation
  - 150+ Orgs
  - GSA
  - Internet2
- Evaluation
  - EU WP-29
  - FSTC
  - GSA e-Authentication
- Adoption
  - EduMart
  - e-Learning
  - Radicchio Ltd.
  - m-Commerce



Gary Ellison

gary.ellison @ sun.com

Buy “Inside Java 2  
Platform Security 2<sup>nd</sup>  
Ed.”

ISBN: 0201787911

