

Web Services Security: Access Control

John Merrells, Director,
Parthenon Computing Ltd.
XML 2004, 16th November 2004

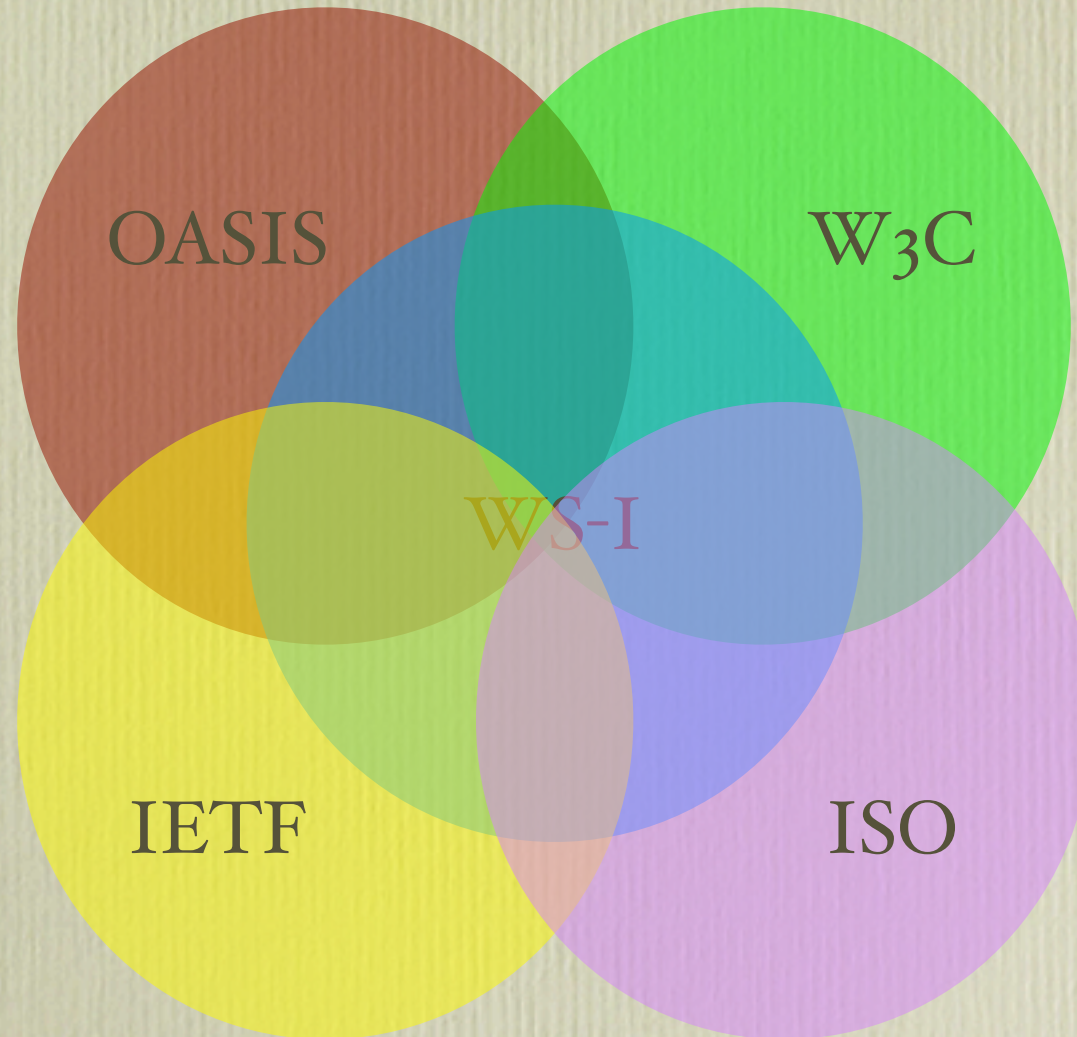
Agenda

- Theoretical Security Framework
- Web Services Security Standards
- Access Control for Web Services

Theoretical Security Framework

- Integrity - ensuring that the message has not been tampered with.
- Confidentiality - ensuring that only the intended recipient can read the message.
- Authentication - establishing identity.
- Authorization - establishing what an identity can do.

Web Services Standards



Web Services Interoperability

- Basic Security Profile
 - Security Challenges
 - Peer and Data Origin Authentication
 - Data Integrity for Transport and Message
 - Data Confidentiality for Transport and Message
 - Message Uniqueness

Transport Level Security Options

Challenge Supported	Transport Layer Technologies used	
Integrity	SSL/TLS	
Confidentiality	SSL/TLS	
Provider Authentication	SSL/TLS	
Consumer Authentication	SSL/TLS with Client Auth	
	HTTP Basic	
	HTTP Digest	
	HTTP Attributes	
	SSL/TLS	HTTP Basic
		HTTP Digest

Message Level Security Options

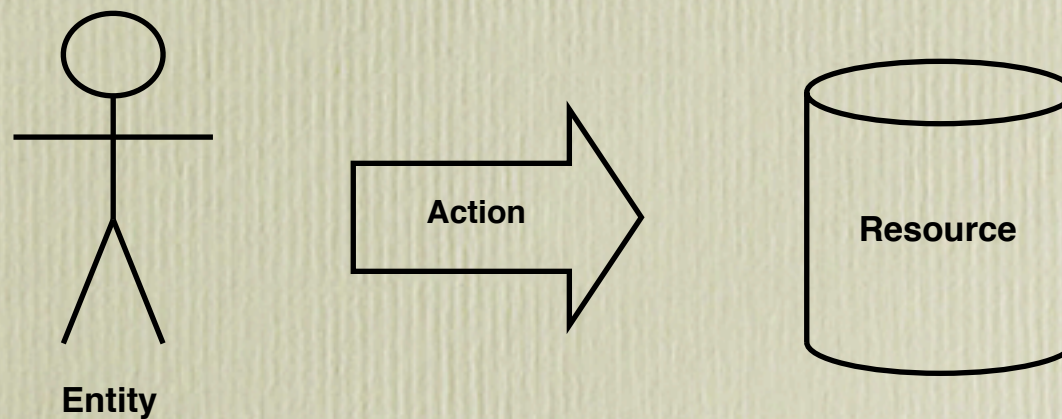
Challenge Supported	Message Layer Technologies used	
Integrity	XML Signature	
Confidentiality	XML Encryption	
SOAP Sender Authentication	XML Encryption	username and [password digest]
	username and [password digest]	
	X.509 Certificate	
	Kerberos Token	

Message Level Security Options

- XML Encryption, W₃C, December 2002
 - Provides data encryption.
- XML Signature, W₃C, February 2002
 - Provides integrity, message authentication, and/or signer authentication.

Authorization

- Authorization is the permission for an entity to perform some action against some resource.



Web Services Standards

- OASIS Technical Committees
 - Authentication
 - Web Services Security (WS-Security)
 - Authorization
 - eXtensible Access Control Markup Language (XACML)
 - Security Protocol
 - Security Services (SAML)

Web Services Security

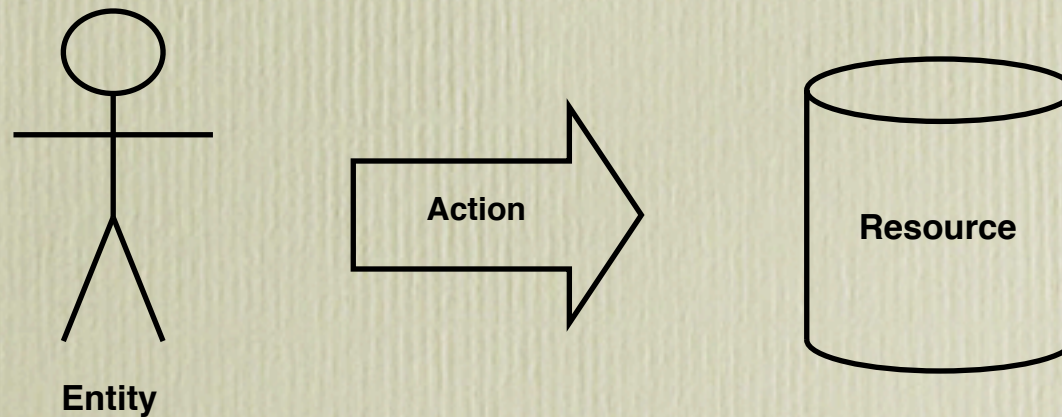
- SOAP Message Security V1.0, March 2004
- Token Profiles
 - Username Token Profile V1.0, March 2004
 - X.509 Token Profile V1.0, March 2004
 - REL Token Profile, Draft, June 2004 [NEW]
 - SAML Token Profile, Draft, July 2004 [NEW]

XACML

- ‘eXtensible Access Control Markup Language’
- It describes...
 - Access Control Language
 - Processing Environment
 - Request / Response Protocol

Access Control Language

- An Access Control Rule identifies an entity, an action and a resource and says if the action is allowed or not.
- XACML Language: Types, Operations, Functions, Collections.



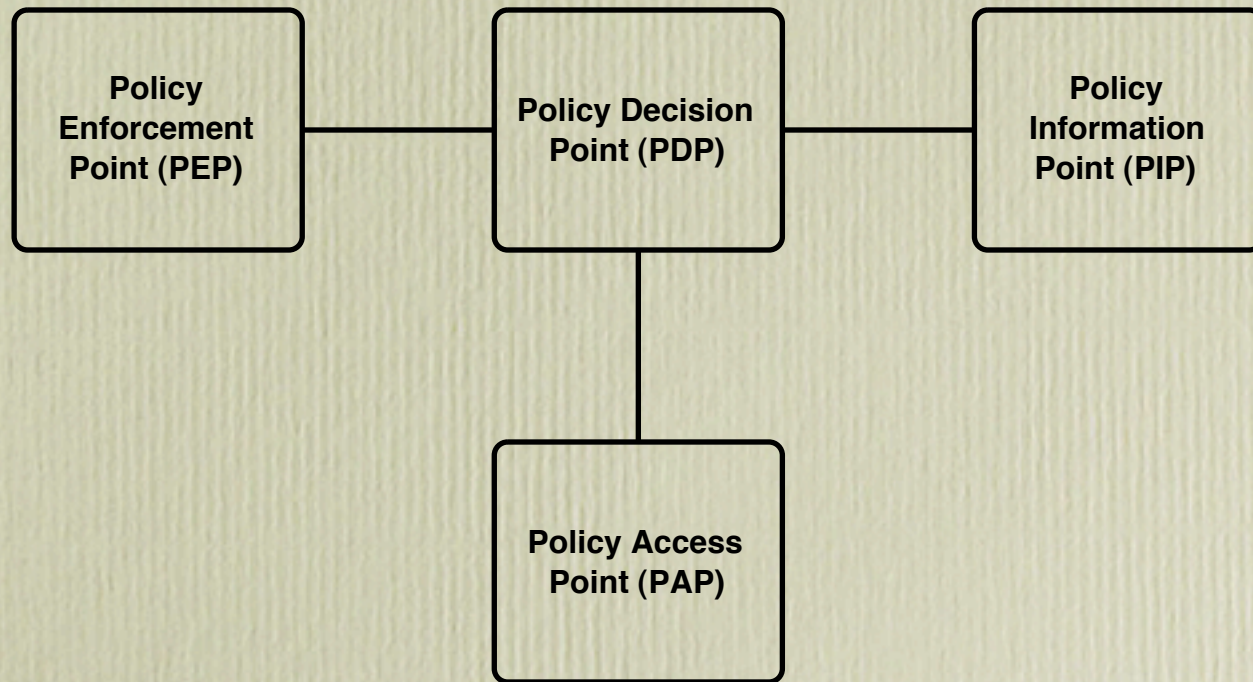
Example Access Control Rule

- Permit 'John' to 'Open' the 'Door'
 - Entity: 'John'
 - Action: 'Open'
 - Resource: 'Door'

Example XACML Rule

- ```
<Rule RuleId="" Effect="Permit"> <Description>Permit John to Open the Door</Description>
<Target>
 <Subjects><Subject>
 <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">John</AttributeValue>
 <SubjectAttributeDesignator
 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
 DataType="http://www.w3.org/2001/XMLSchema#string"/>
 </SubjectMatch>
 </Subject></Subjects>
 <Resources><Resource>
 <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">door</AttributeValue>
 <ResourceAttributeDesignator
 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
 DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
 </ResourceMatch>
 </Resource></Resources>
 <Actions><Action>
 <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">open</AttributeValue>
 <ActionAttributeDesignator
 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
 DataType="http://www.w3.org/2001/XMLSchema#string"/>
 </ActionMatch>
 </Action></Actions>
</Target>
</Rule>
```

# Processing Environment

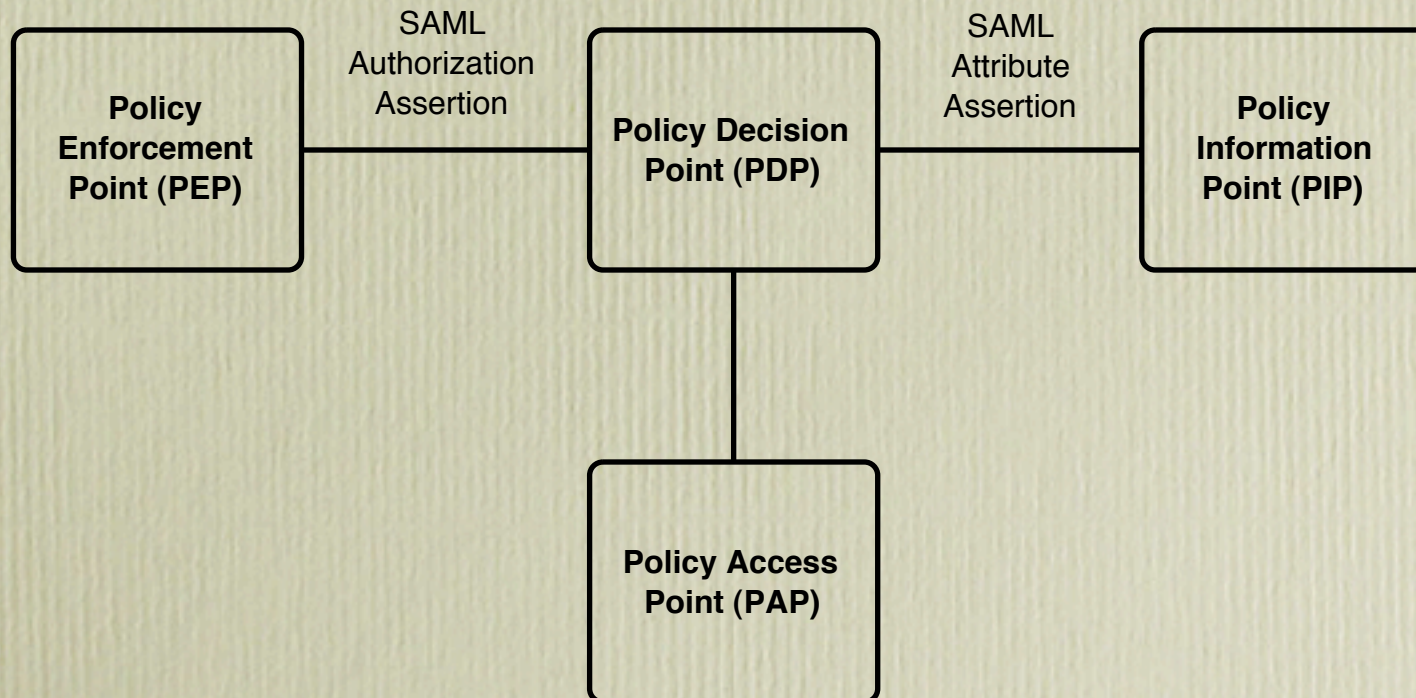


# Request/Response Protocol

- XACML Request
  - Entity
  - Action
  - Resource
- XACML Response
  - Permit
  - Permit with Obligations
  - Deny
  - Not Applicable
  - Indeterminate

# SAML

- ‘Security Assertions Markup Language’
- Assertions for Authentication, Authorization and Attributes.

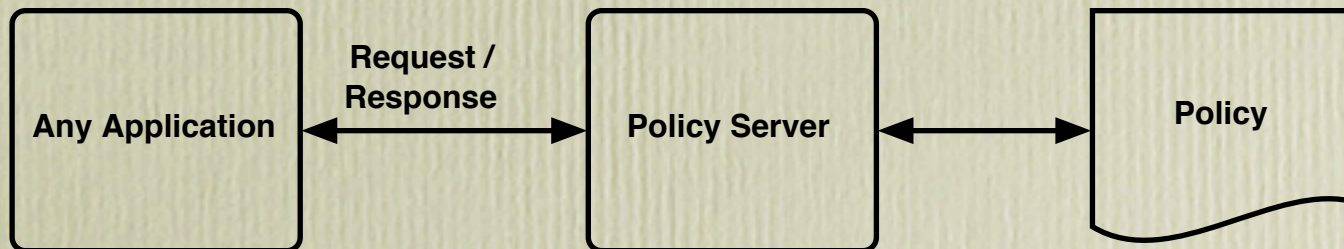


# Access Control for Web Services

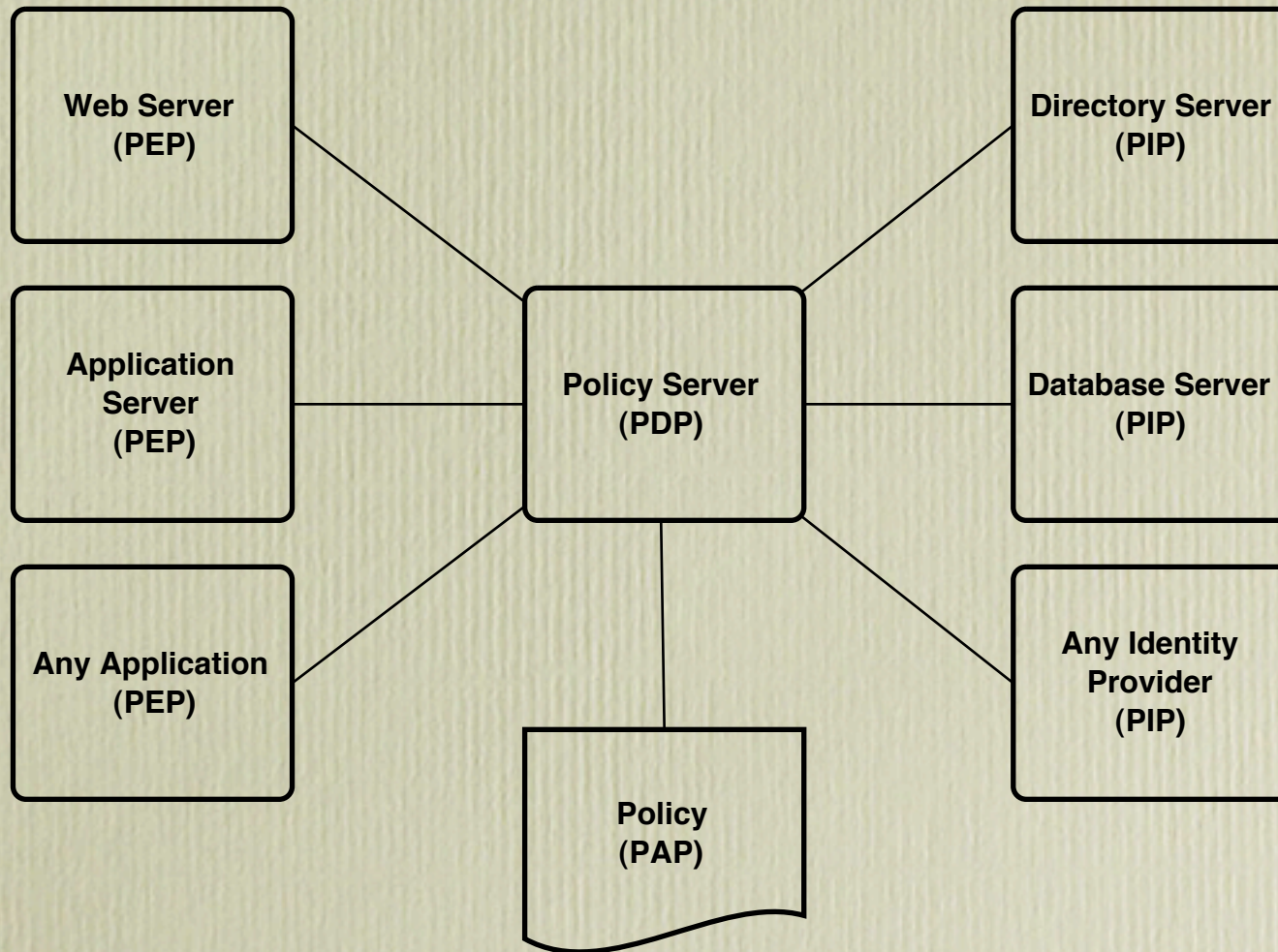
- Solutions
  - A XACML/SAML enabled...
    - Policy Server, or
    - Firewall.
  - Web Services Security Policies in XACML

# Policy Server

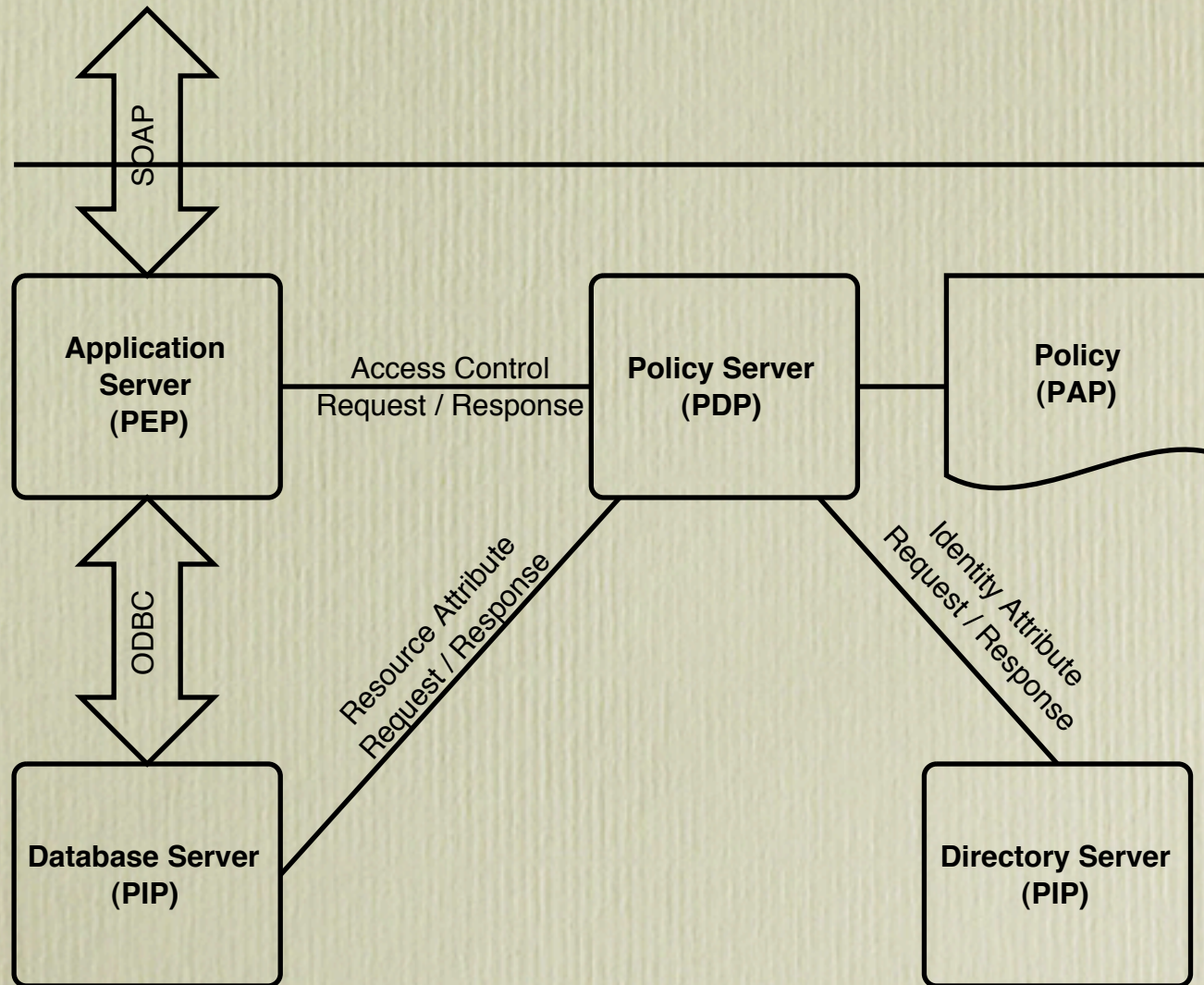
- The Policy Server accepts Access Control Requests, processes them against a Policy and returns an Access Control Response.
- A Policy is the set of Access Control Rules that drive a policy server.



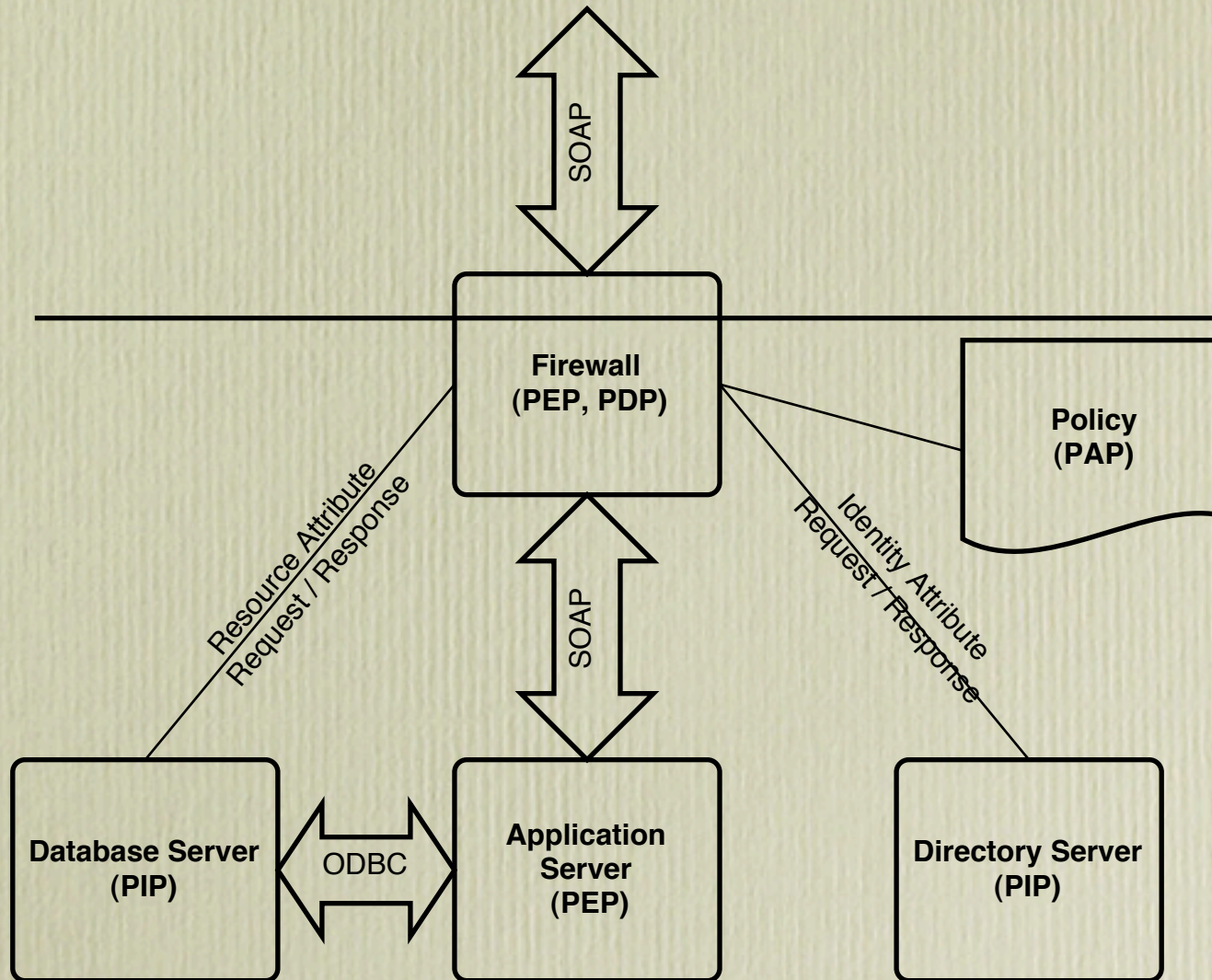
# Policy Server Environment



# Policy Server Deployment



# Firewall Deployment



# XACML and Web Services

- Web Services Policy Language (WSPL)
  - ‘Web-services policy language use-cases and requirements’, Draft, April 2003
  - ‘XACML Profile for Web Services’, Draft, September 2003
    - Resource: End-Point
    - Action: Method Call
    - Entity: Process, User

# Technology Providers



# Parthenon Computing Ltd

- A Software Engineering Consultancy
- John Merrells, Director, Founder
- Gareth Reakes, Director, Founder
- Nine Full-Time Engineers
- Offices at The Oxford Centre for Innovation
- Privately Held. Self Funded.

# For More Information

- Parthenon Computing Website
  - <http://www.parthcomp.com>
- Download the XACML Policy Test Tool
  - <http://www.parthcomp.com>
- Talk to John Merrells,
  - [merrells@parthcomp.com](mailto:merrells@parthcomp.com)

# Future Work

- WS-Trust
- WS-SecureConversation
- WS-Policy
- WS-PolicyAttachment
- WS-PolicyAssertions
- WS-Addressing
- WS-ReliableMessaging
- WS-Federation

# XACML 2.0

- Profiles
  - Digital Signature, Hierarchical Resources, LDAP, Privacy, RBAC, SAML Integration
- Condition and Rules References
- Combining Algorithm Parameters
- Environment in Target
- Time in Range
- Policy Versions
- Negative Target Match
- New Functions

# XACML 3.0

- Administrative Policies
- Policy delegation
- Configuration Metadata
- Domain Specific Identifiers
- Function Declarations
- Missing Attributes