

# Identity & Policy (for Security, Privacy and Trust)

March, 4<sup>th</sup> 2008

NIST

Identity and Trust Symposium

Rakesh Radhakrishnan

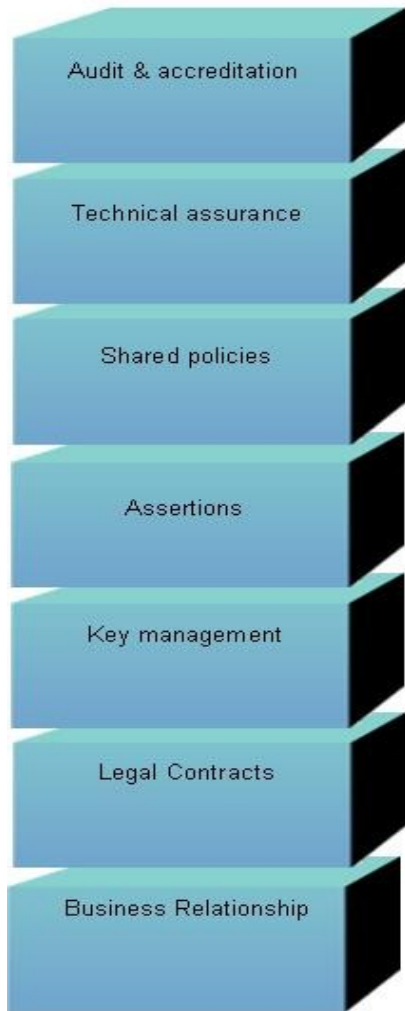
Chief Identity Integration Architect (Telco)

Sun Microsystems, Inc.

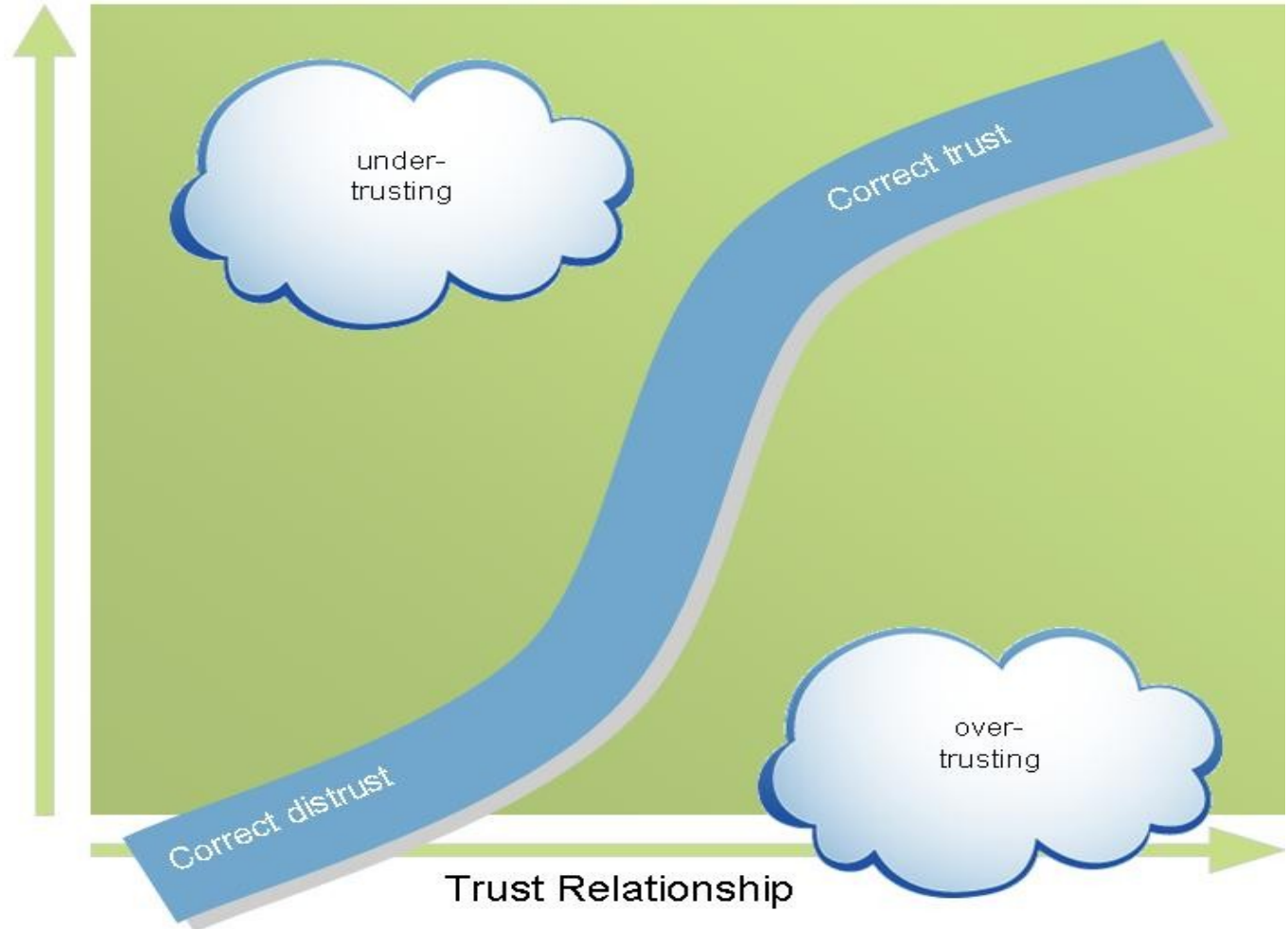
# Agenda

- Vertical Integration of Identity Systems (mapping identifiers and aggregating meta-data)
- Policy based Security Service invocation (SaaS)
- Pervasive Policy Paradigm
- FAM Policy System Architecture
- Policy Orchestration (papers + POC/Pilots and Prototypes)

# Identity and Trust



Building Blocks



# Identity and Trust

## Technical Assurance

(ID Assurance, Reputation,  
Aligning with NAC, HSS, TPM,  
Resource specific tools, etc.)

## Auditing

(log management, regulatory  
compliance, accreditation, reporting,  
non-repudiation, forensics, etc)

## Shared Policies (PPP)

(PEP, PDP, PMP, PCCP, PIP, etc.)

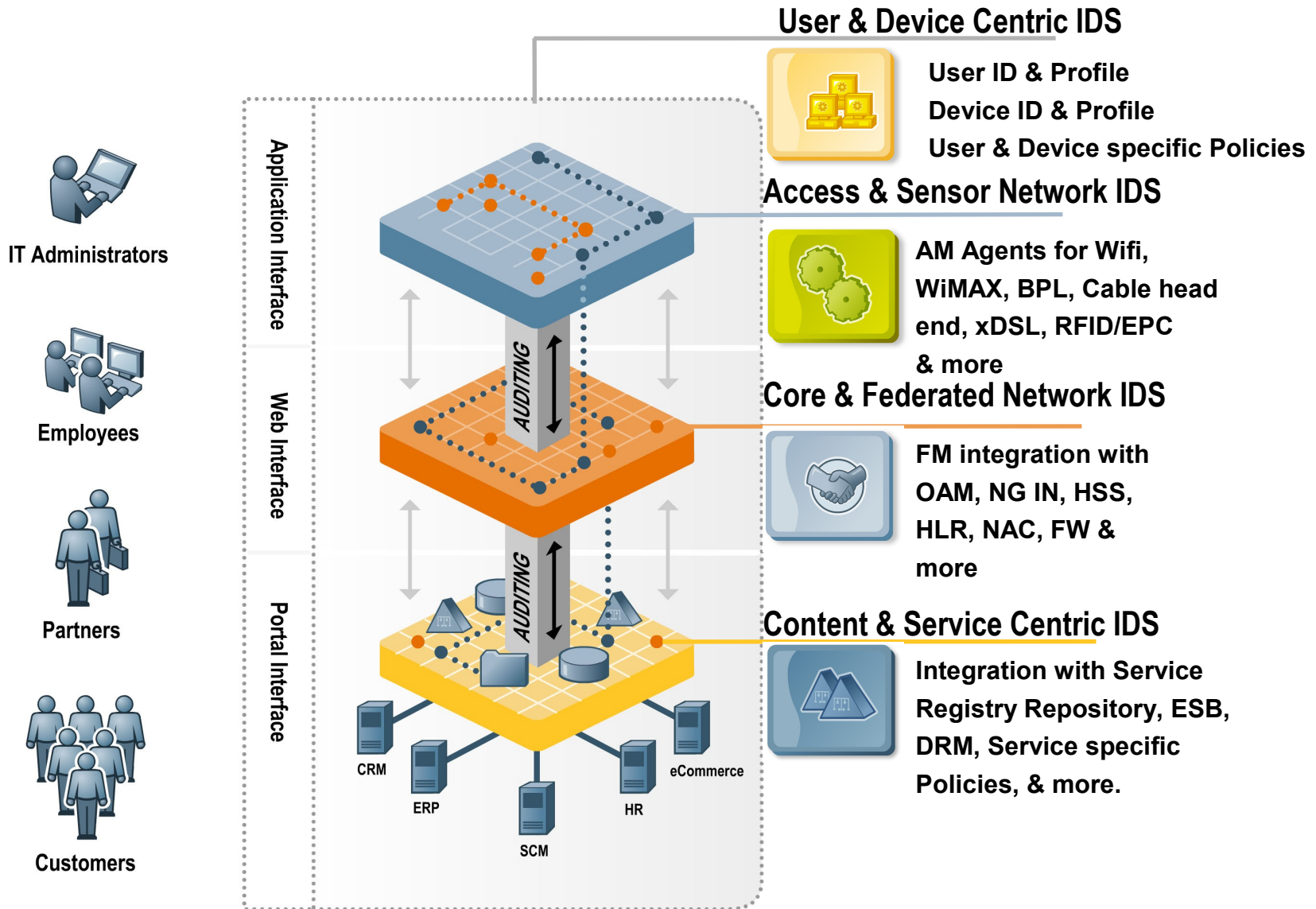
## PKI

(TLS/SSL based Open-SSL,  
3<sup>rd</sup> party CA,  
& types of PKI -X.509 & PKIX)

## Assertions

(SAML, XACML,  
other attributes, etc.)

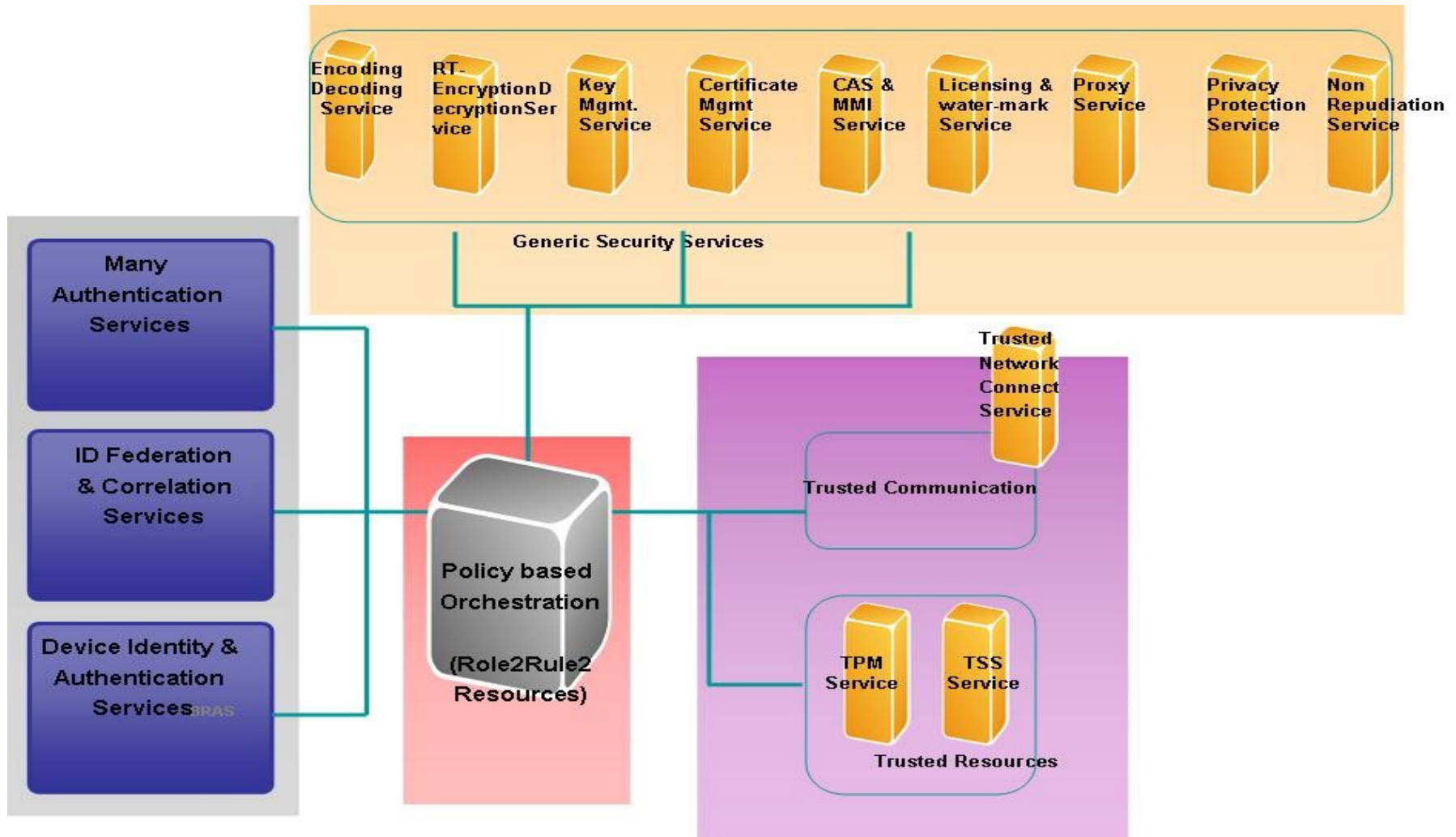
# Vertical Integration (Identity & Security)



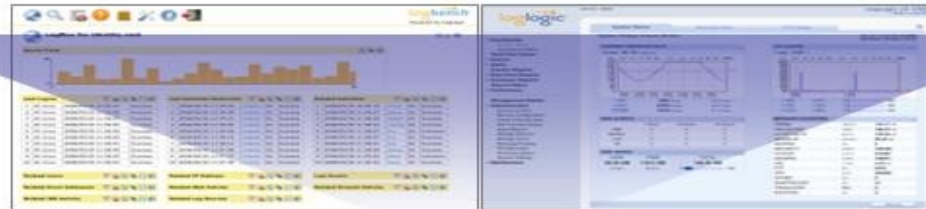
# Policy based Security Services (SAAS)

- **Authentication Services (many Authentication types/contexts)**
- **Policy Services (Rule Management Services)**
- **Federation Services (CDSSO, COT, interlinked Federation)**
- **Session Services (distributed sessions – network facing and service facing)**
- **Logging Services (end to end)**
- **Token Management Services (token table, token transfers, etc.)**
- **Repository Services (agnostic to repository technology)**
- **Key Management Services (certificates, algorithms, enc/dec)**
- **Identity Reputation Services (history of transactions)**
- **Identity Assurance Services (NIST/Liberty)**
- **Identity and Trusted Computing (Resource labeling+TPM)**
- **Identity Privacy Management Services (icons)**
- **Role Management Services (full life cycle of roles)**
- **Identity Context Services (location, presence, etc.)**
- **Identity Mobility Services (roaming, distributed sessions, etc.)**
- **Identity Service Management Services (service provisioned to entities)**
- **Identity DRM Services (disintermediation)**
- **Identity Audit and Compliance Services (reporting)**

# Policy based Security Services (SAAS)



# Pervasive Policy Paradigm



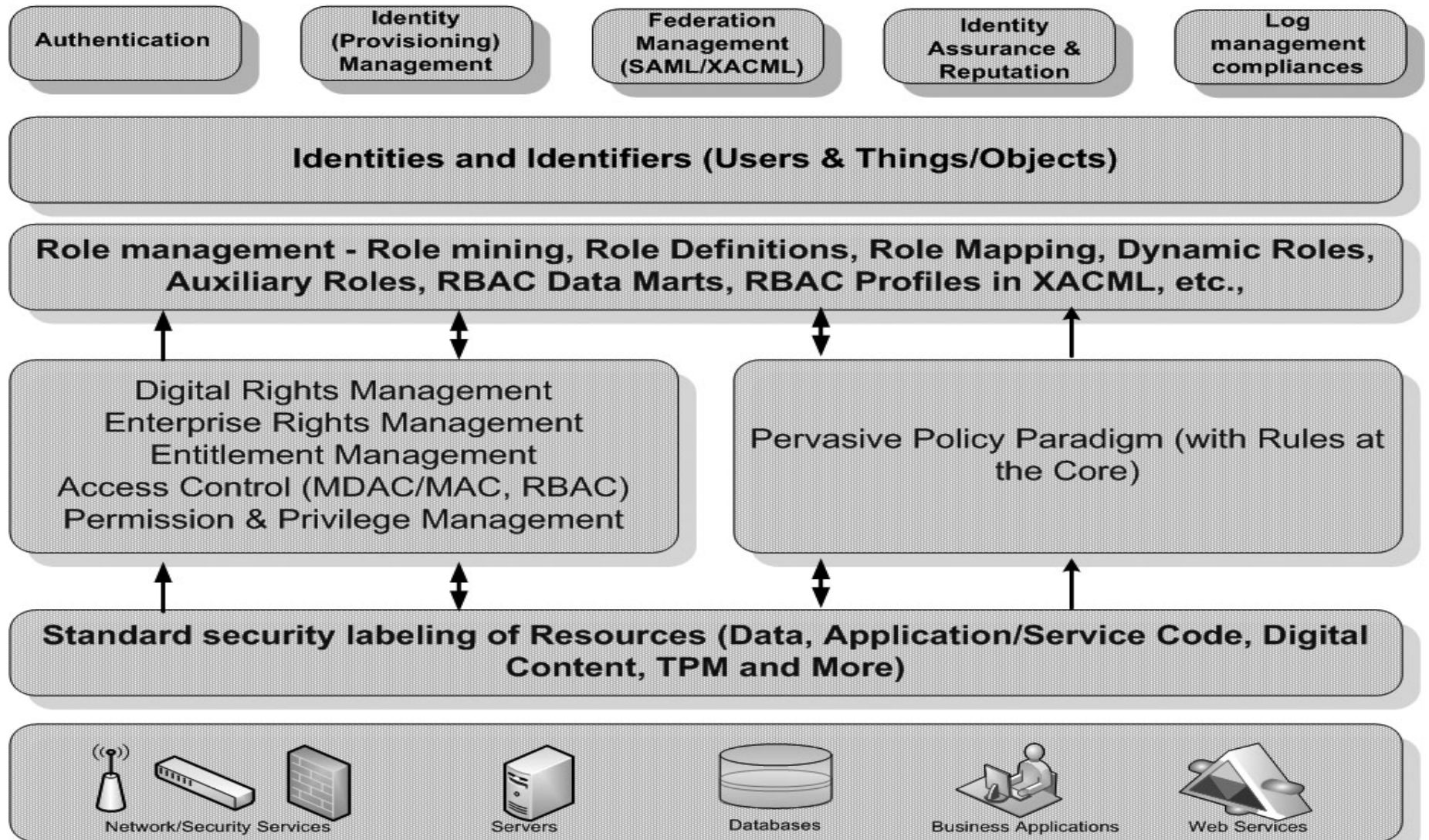
**Policy Set Executing Rules from a Repository**  
 (Aligned to Identities & Identifiers –transient and persistent)  
 Rules around privileges, permissions, rights, access control, & more)

Resource Classification, Compartmentalization and Labeling

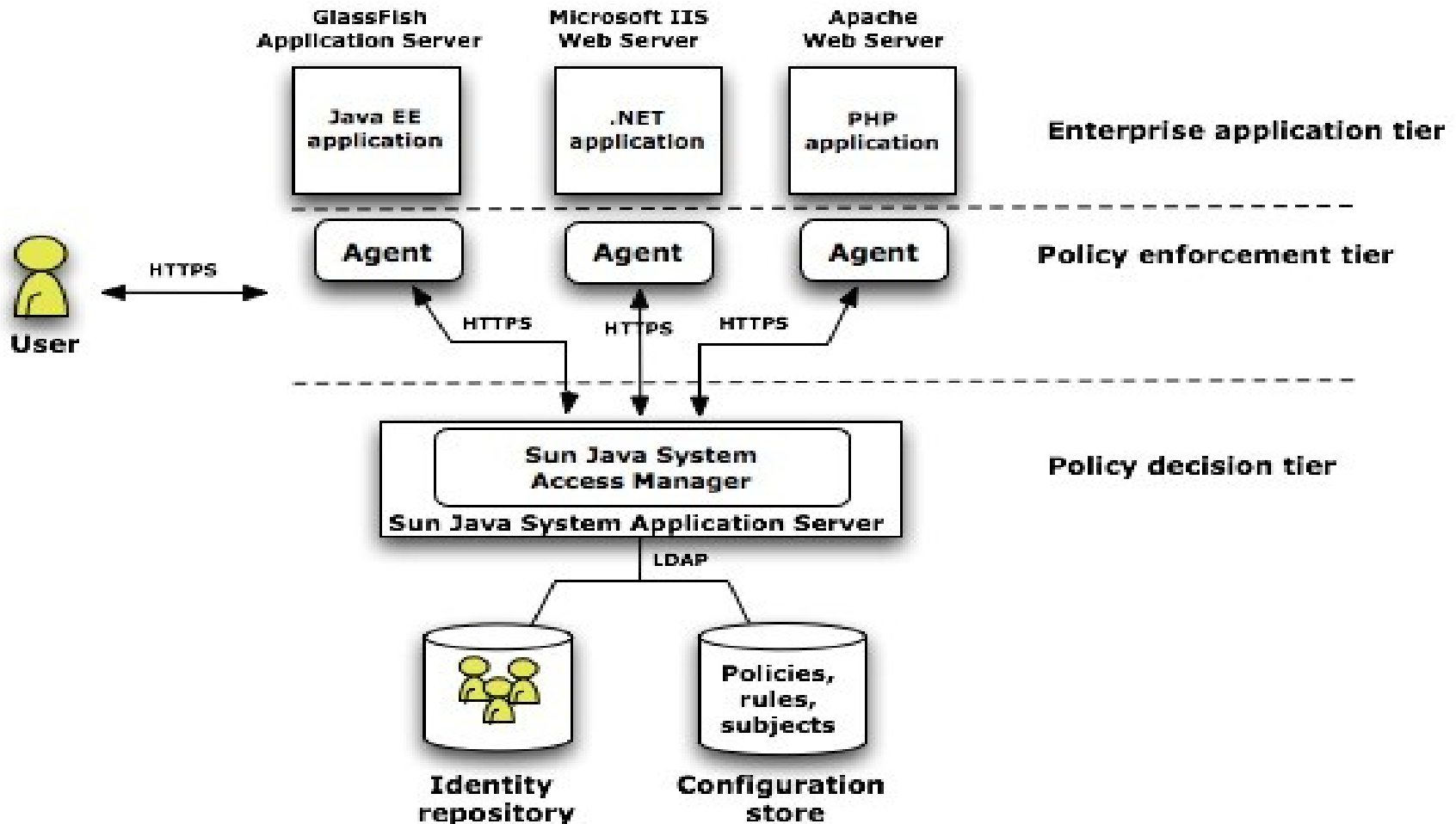


Rules that ensures appropriate security services are leveraged (encryption, certificate/ keys, token mgmt, scrambling, licensing, reputation mechanism, protocols, label mgmt, platform security modules (TPM, TNC, TC), etc.

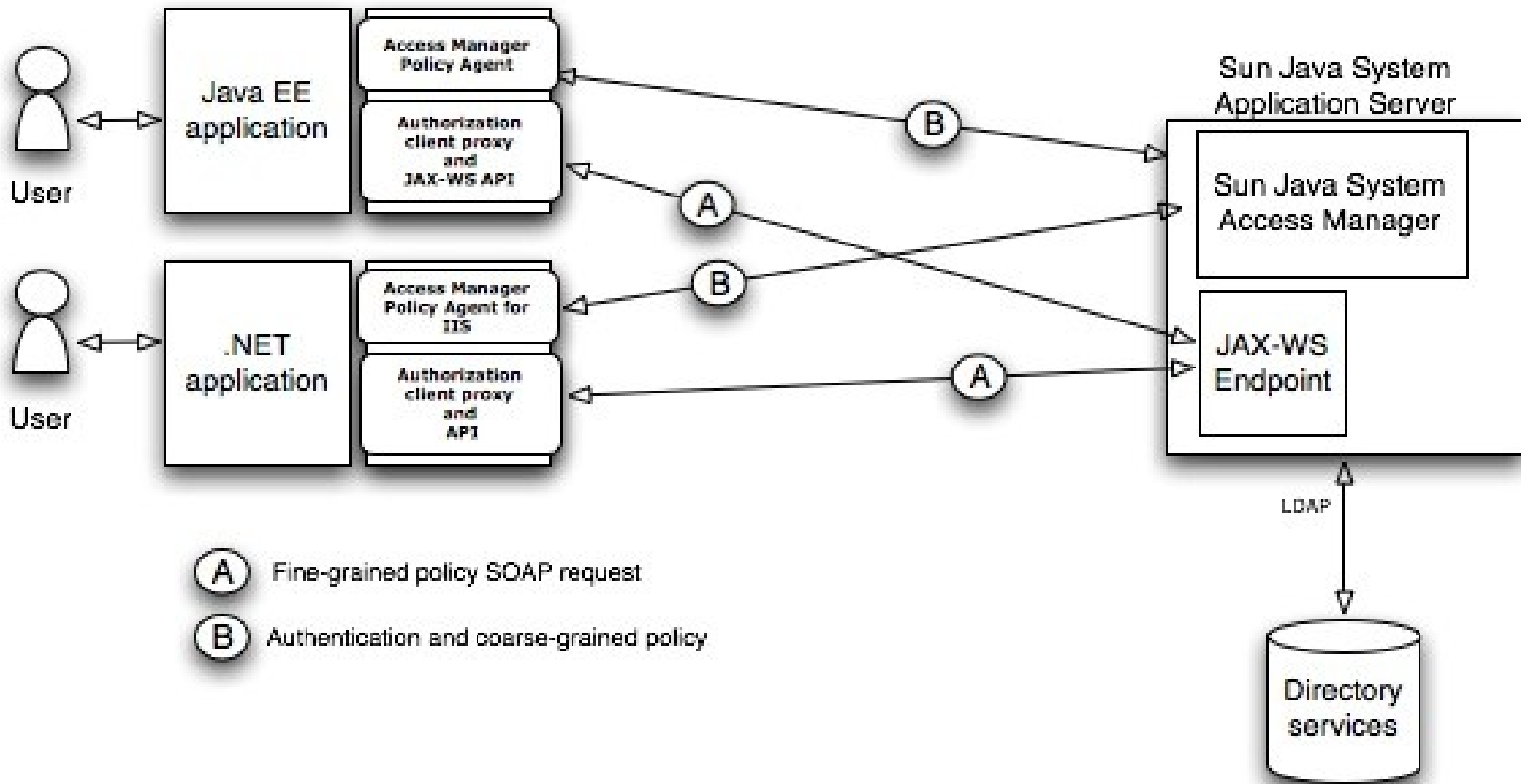
# Pervasive Policy Paradigm



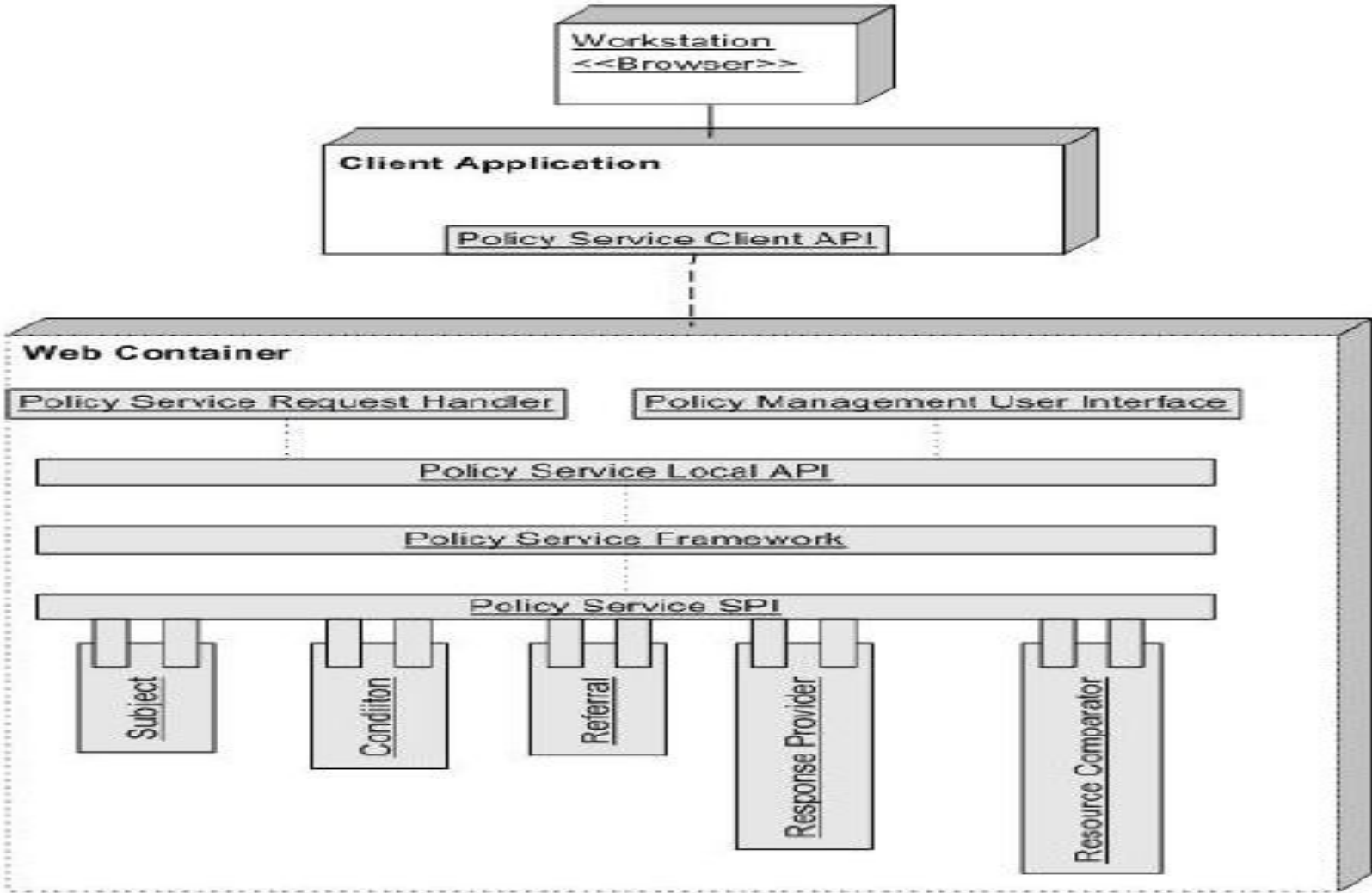
# Pervasive Policy Paradigm



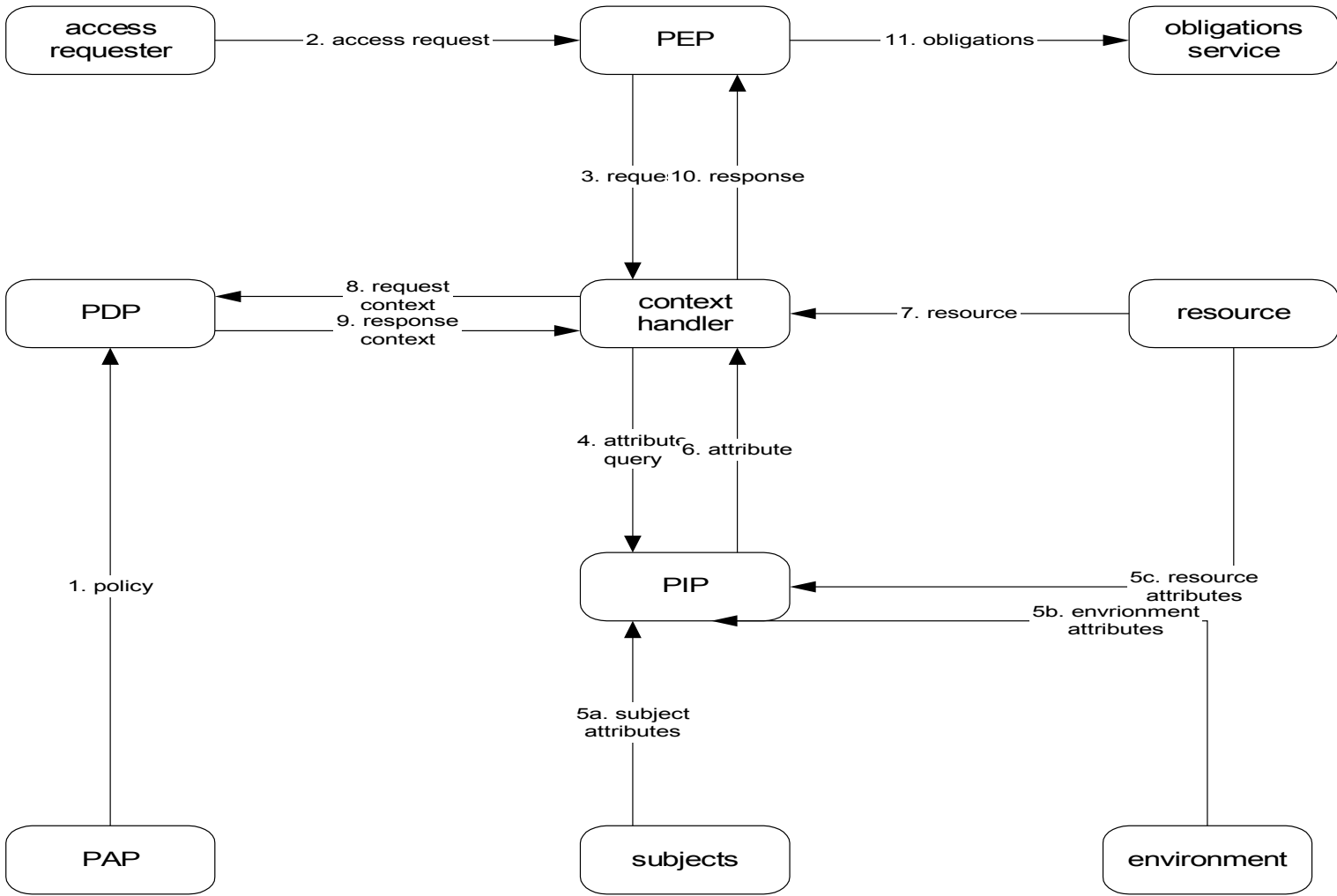
# Pervasive Policy Paradigm



# Policy System for SOA (FAM 8.x Architecture)



# Policy System for SOA (FAM 8.x Architecture)



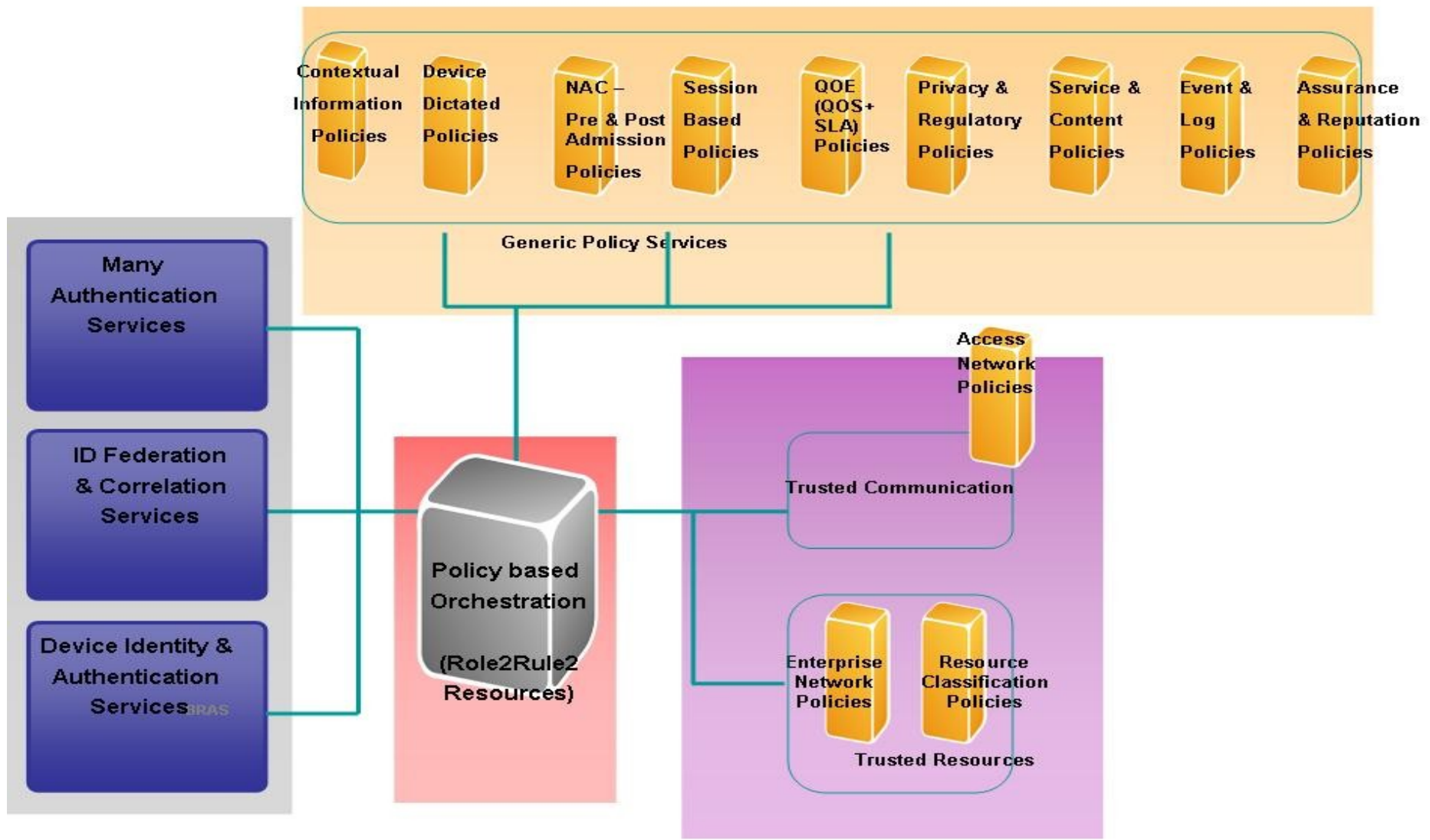
# Pervasive Policy Paradigm

- To provide a method for combining individual rules and policies into a single policy set that applies to a particular decision request
- To provide a method for flexible definition of the procedure by which rules and policies are combined
- To provide a method for dealing with multiple subjects acting in different capacities
- To provide a method for basing an authorization decision on attributes of the subject & resource
- To provide a method for dealing with multi-valued attributes
- To provide a method for basing an authorization decision on the contents of an inf resource
- To provide a set of logical and mathematical operators on attributes of the subject, resource and environment
- To provide a method for handling a distributed set of policy components, while abstracting the method for locating, retrieving and authenticating the policy components
- To provide a method for rapidly identifying the policy that applies to a given action, based upon the values of attributes of the subjects, resource and action
- To provide an abstraction-layer that insulates the policy-writer from the details of the app env
- To provide a method for specifying a set of actions that must be performed in conjunction with policy enforcement

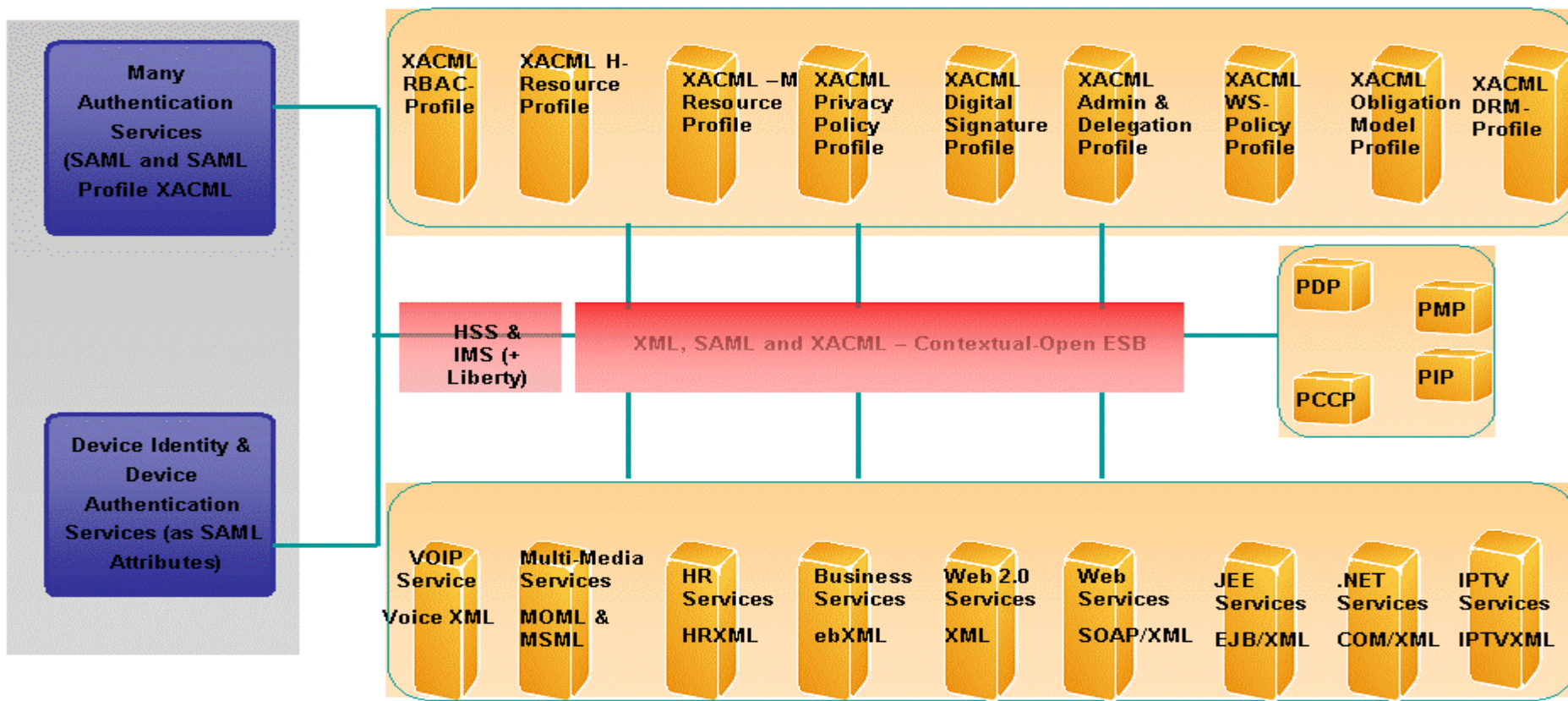
# Pervasive Policy Paradigm

- Identity enabled Derived Device Policies
- Identity enabled Access Networks Policies
- Identity enabled QOS/QOE Policies
- Identity enabled Session Specific Policies
- Identity enabled Privacy Preservation Policies
- Identity enabled Service Security Policies
- Identity enabled Content Control Policies
- Identity enabled Enterprise Network Policies
- Identity enabled Regulatory Requirement Policies
- Identity enabled Event Log Policies
- Identity enabled Contextual Policies
- Identity enabled Policy Assurance (with PCCP)
- Policy Orchestration

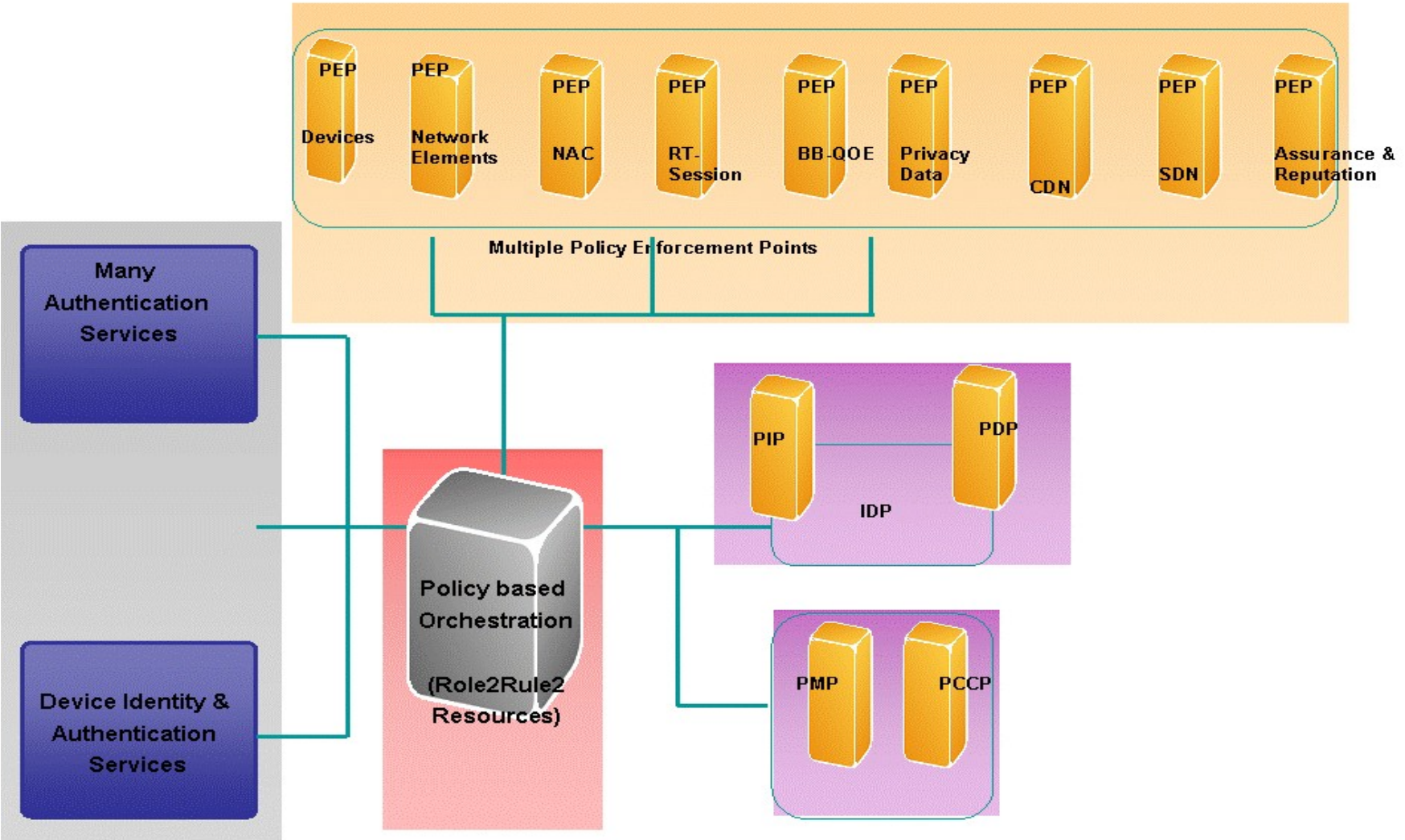
# Policy Orchestration for Control & Alignment



# Policy Orchestration using XML & XACML



# Policy Orchestration for Control & Alignment



# 100+ XACML Papers & Series

- NIST Paper on Device & Log Policies (PDA or any Mobile IP Devices)
- NCSA Paper on Policies for VO (PIP and PCCP)
- Dr. Mouli's papers on RBAC/XACML, Privacy Policies, Enterprise Policies and Policy Inference (4 papers)
- Papers on Contextual Policies and Mobile Agents
- Joint papers with ISV, NEP & Industry Forum
  - Book 1: Identity and Security (06/07)
  - Book 2: Identity and Policy (06/08)
  - Book 3: Identity and SOA -09 (context, mobility, Enterprise SOA, etc.)
  - Book 4: Identity and Trust -09 (TCG, TPM, COT, TNC, etc.)
  - Book 5: Identity and eGov 10 (Assurance and Reputation)

# 100+ POC, Pilot and Proto-types

- Cisco, Juniper, Alcatel, Nokia/Siemens and many more NEP's integrate with FAM for NAC policies
- Trust Digital and I-Ovation like ISV's for Device policies
- TAZZ & Bridge-water for BB 4G Networks for IMS, IPTV policies
- Kabira and Telcordia for RT-Charging Policies (session based policies)
- True-baseline, Cisco and Juniper for QOS policies
- Layer 7 Technologies for Service policies
- Reactivity and Securent for Enterprise Network policies
- Log Logic for Event and Log Policies
- CDN policies (projects)
- OSS/BSS TMF Co-op and policy orchestration
- I-pass for Network facing policy orchestration
- Sun ESB and FAM for service policy orchestration

# What did we learn?

- XACML is great for abstraction of policies and Attributes (ABAC) -service orchestration automatically invokes polices
- Policies themselves require operator or user defined workflow (e.g., device + NAC + user level authN -iPass)
- Continuity in end point security (event based Policies)
- RT Policy Checking and Certification is very important (PCCP) requires orchestration
- Policy Information Point can leverage XDI (PIP) and can share context via an Open ESB
- Use-full for aligning Service SLA with Network QOS
- Changes in Environment (code RED, breaches in the network, etc.) forces dynamic policy work-flows
- Alignment to Audit Rules and Log based Policies
- Session Specific policies invoked when highly Security Sensitive Service is invoked.

# What did we learn?

- Stage 0 – Registration is Key for Success – this includes identity provisioning, role management and rule definitions, workflow definitions, etc.
- Do not forget things like -Support multiple password policies for a user, depending on the targets on which he is having account etc.
- RBAC is a project by itself
- POC and Demo's when followed up with Real Projects require Executive Sponsors, Resources (SI, Partners), and a methodology
- Most projects are JEE environments with Heterogeneous platforms
- Not all XACML profiles will be leveraged for initial stages of project – resource profile with request response works well for most use cases (H and M), RBAC profile is extremely power full, XACML –WS policy has been used, privacy policy exchange tested, QOS policies trialed.
- Plan for acquisitions and mergers impacting project

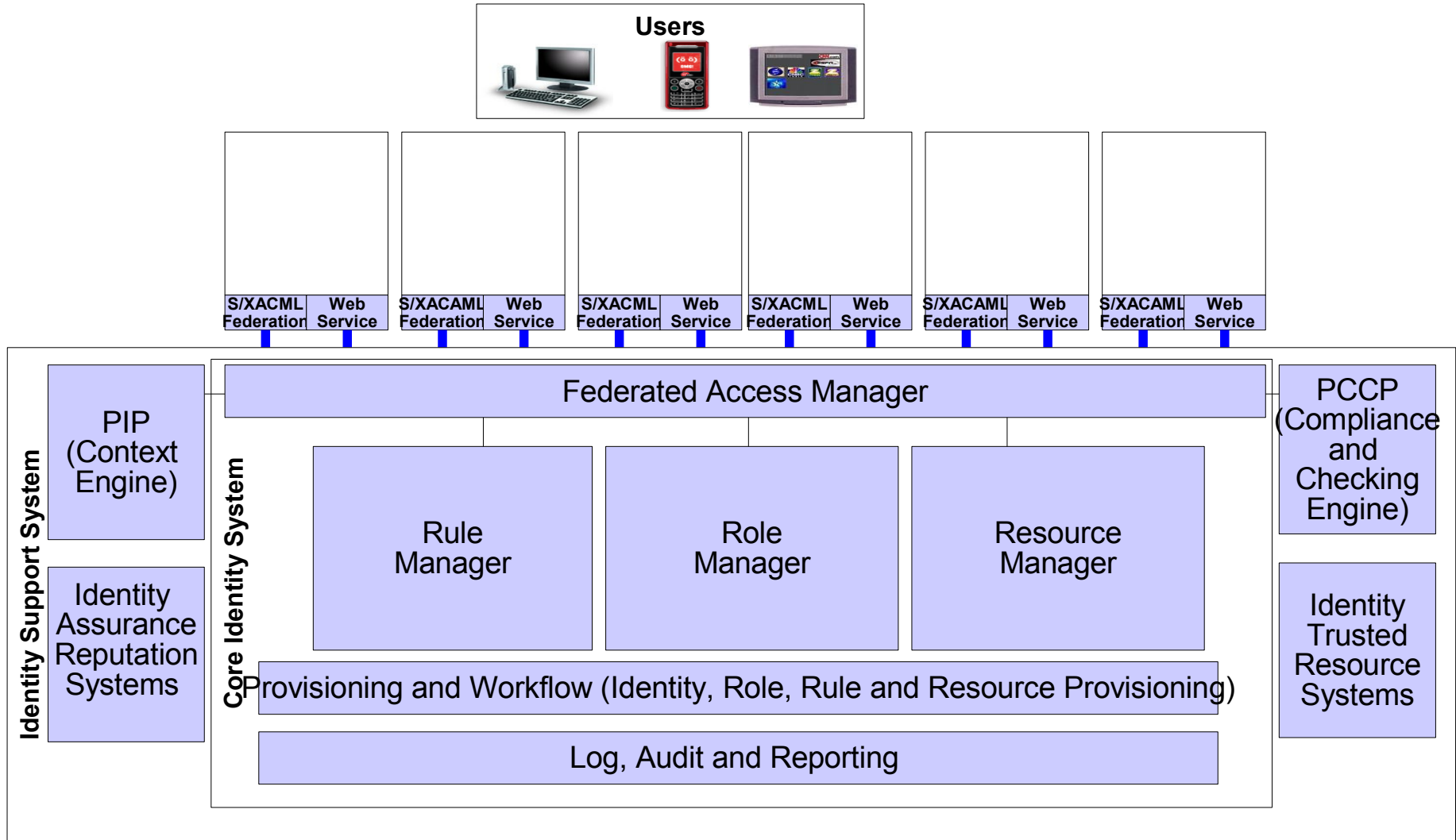
# What did we learn?

- Policy Orchestration works – not all use cases require end to end orchestration – but will require a subset of policies to be orchestrated – NAC policy, Device Policy and AuthN policy for example – with the Req-Resp model between multiple PEP and PDP's
- PIP integration is basically Secure Exchange of Context Data and Profiles (location, presence, preference, etc.)
- Policies are integral part of Identity Assurance
- PCCP – Policy Compliance and Checking points external to a PMP will be required for ongoing continuous validation of legitimacy of policy with inference and other techniques
- XACML –DRM ? Abstraction from multiple DRM techniques
- Delegation and Administration profile in a PMP (3<sup>rd</sup> party)
- Obligation (3<sup>rd</sup> party)

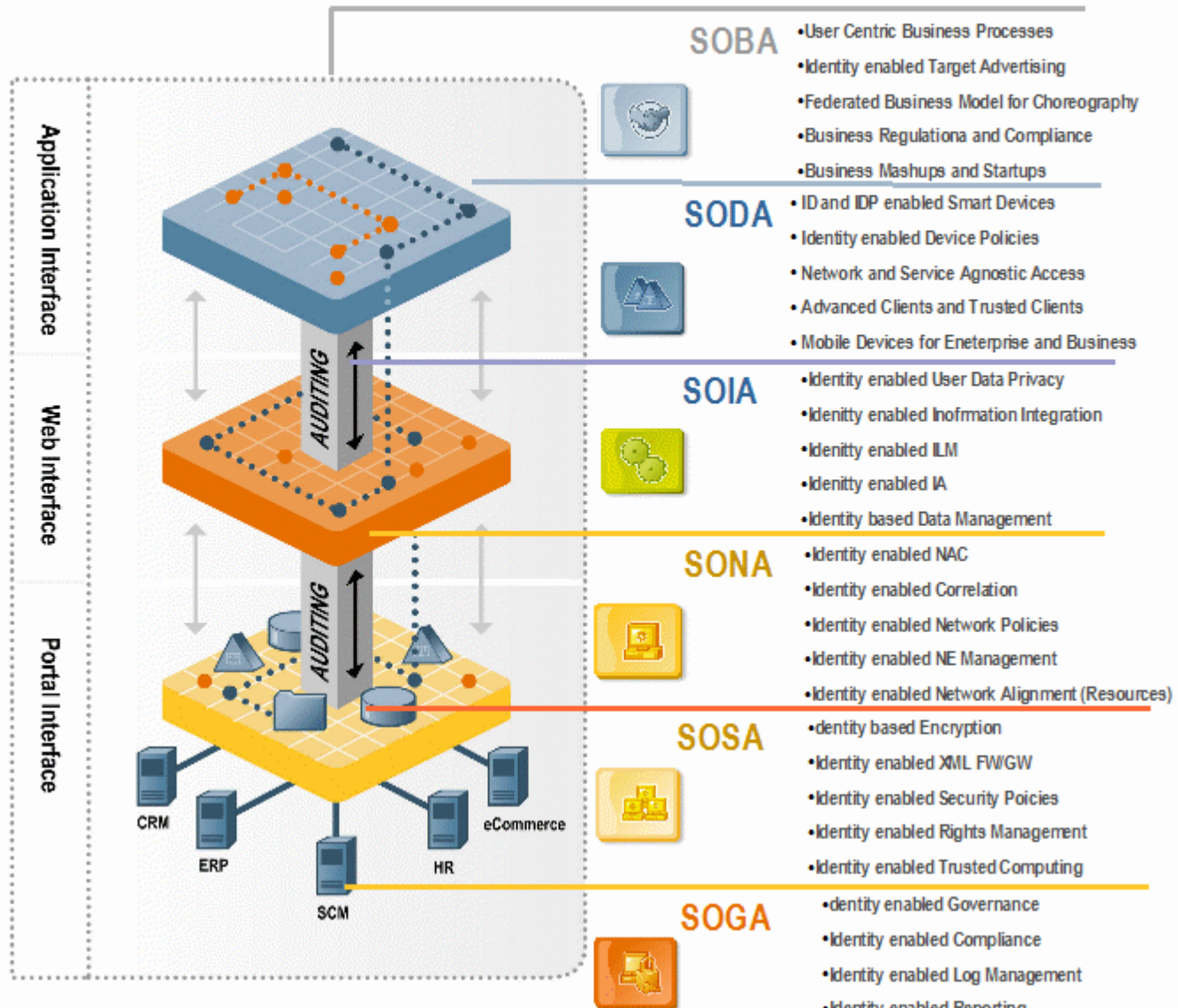
# What did we learn?

- Its not easy – The tools are there – but it requires extensive discipline and Project Management
- Each project is driven by specific domain level requirements (Privacy and Audit or QOE)
- Partners are extremely important for creating an Eco System
- POC and Proto-type in a Lab is a different project from Production (Architecture Assessment helps and Pilots as well)
- Leverage Speciality integration partners
- Address scope with phases (1 to 5)
- Create Policy Building Blocks (with XACML abstraction)
- Align with Role Management, Resource Management and SOA projects
- Policy Infrastructure is key for ID Governance

# An evolving Identity System



# Identity System – An Axel for Alignment



# Thank You !!!

*[rakesh.radhakrishnan@sun.com](mailto:rakesh.radhakrishnan@sun.com)*

*<http://www.network-identity.com>*