Identity & Policy
(for Security, Privacy and Trust)

October 28th, 2008
Liberty Alliance Wrbcast

Rakesh Radhakrishnan
Principle Architect (Telco)
Technology Lead (Telco)
Sun Microsystems, Inc.
Agenda

• Integration Perspectives of Identity System
• Policy based Security Service invocation (SaaS)
• Pervasive Policy Paradigm
• FAM Policy System Architecture
• Policy Orchestration (papers + POC/Pilots and Prototypes)
Identity System

Core Identity System

Federated Access Manager

Rule Manager

Role Manager

Resource Manager

Provisioning and workflow (Identity, Role, Rule and Resource Provisioning)

Log Audit and Reporting

Identity Support System

Identity Assurance Reputation Systems

PIP Context Engine

PCCP Compliance Checking Engine

Identity Trusted Resource Systems
Integration Perspectives

- OTP AuthN
- Axsonics 3factor AuthN
- Aware biometric AuthN
- ActivIdentity and Strong AuthN
- SIM based Authentication
- Cardspace AuthN for MS environments
- Digest AuthN for SIP environment
- GBA/GAA based AuthN for HSS/IMS environment
- HTTP transport level AuthN (JBI/ESB) for SOA
- OpenID Extensions
- Kerbeorus AuthN
Integration Perspectives

- Identity enabled Contextual/User Policies
- Identity enabled Device Policies
- Identity enabled Access Network Policies
- Identity enabled Session specific Policies
- Identity enabled Privacy Policies (Consumer and Corporate)
- Identity enabled QOS Policies
- Identity enabled Regulatory Policies
- Identity enabled Service centric Policies
- Identity enabled Content control Policies
- Identity enabled Enterprise Network Policies (Securent/NAC)
- Identity enabled Log Policies (Log Logic and SignaCert)
- Identity enabled Assurance Policies (Assurance Levels)
Integration Perspectives

> Federated Identity + Federated Policy leads to Federated Context
> Federation acts as the Conduit that Conveys and Carries Context
> NEP's Nortel (Sican), Ericsson and others are creating Engines
> Invaluable for 4G broadband networks
> Context Areas
  > Enterprise Networks and Role based Context
  > Social Networks and Persona driven Context
  > Personal Networks and Profile/Preferences Context
  > Mobile Networks and Spatial (loc, presence) Context
  > Sensor Networks and Environmental Context
Integration Perspectives

> Integrated with Identity Manager
> Integrated with Role Manager
> Integrated with Compliance Manager
> Integrated with Application Server & ESB
> Integration with SIEM tools in the Market
  > (LogLogic, Prism Microsystems, etc)
Vertical Integration (Identity & Security)

User & Device Centric IDS
- User ID & Profile
- Device ID & Profile
- User & Device specific Policies

Access & Sensor Network IDS
- AM Agents for Wifi, WiMAX, BPL, Cable head end, xDSL, RFID/EPC & more

Core & Federated Network IDS
- FM integration with OAM, NG IN, HSS, HLR, NAC, FW & more

Content & Service Centric IDS
- Integration with Service Registry Repository, ESB, DRM, Service specific Policies, & more.
Identity and Trust

Building Blocks

- Audit & accreditation
- Technical assurance
- Shared policies
- Assertions
- Key management
- Legal Contracts
- Business Relationship

Correct distrust → under-trusting → Correct trust → over-trusting

Trust Relationship
## Identity and Trust

<table>
<thead>
<tr>
<th>Technical Assurance</th>
<th>Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ID Assurance, Reputation,</td>
<td>(log management, regulatory</td>
</tr>
<tr>
<td>Aligning with NAC, HSS, TPM,</td>
<td>compliance, accreditation, reporting,</td>
</tr>
<tr>
<td>Resource specific tools, etc.)</td>
<td>non-repudiation, forensics, etc)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Shared Policies (PPP)</th>
<th>PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>(PEP, PDP, PMP, PCCP, PIP, etc.)</td>
<td>(TLS/SSL based Open-SSL,</td>
</tr>
<tr>
<td></td>
<td>3rd party CA,</td>
</tr>
<tr>
<td></td>
<td>&amp; types of PKI - X.509 &amp; PKIX)</td>
</tr>
</tbody>
</table>

| Assertions                           |                                               |
|---------------------------------------|                                               |
| (SAML, XACML, other attributes, etc.) |                                               |
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

IT & Operations Users With Relevant Roles
Employees & Partners With Respective Roles
Customers (with Specific Roles)
Users with Privileged Roles

Network Resources
Computing Resources
Data Resources
Services & Custom Apps

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

Identities and Identifiers (Users & Things/Objects)

Role management - Role mining, Role Definitions, Role Mapping, Dynamic Roles, Auxiliary Roles, RBAC Data Marts, RBAC Profiles in XACML, etc.,

Digital Rights Management
Enterprise Rights Management
Entitlement Management
Access Control (MDAC/MAC, RBAC)
Permission & Privilege Management

Pervasive Policy Paradigm (with Rules at the Core)

Standard security labeling of Resources (Data, Application/Service Code, Digital Content, TPM and More)

Network/Security Services, Servers, Databases, Business Applications, Web Services
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

Generic Policy Services

- Contextual Information Policies
- Device Dictated Policies
- NAC - Pre & Post Admission Policies
- Session Based Policies
- QOE (QOS+SLA) Policies
- Privacy & Regulatory Policies
- Service & Content Policies
- Event & Log Policies
- Assurance & Reputation Policies

Policy based Orchestration (Role2Rule2 Resources)

- Many Authentication Services
- ID Federation & Correlation Services
- Device Identity & Authentication Services

Access Network Policies

Trusted Communication

Enterprise Network Policies

Resource Classification Policies

Trusted Resources
Policy Orchestration using XML & XACML

Many Authentication Services (SAML and SAML Profile XACML)

Device Identity & Device Authentication Services (as SAML Attributes)

HSS & IMS (+ Liberty)

XML, SAML and XACML – Contextual-Open ESB

VOIP Service – Voice XML

Multi-Media Services – MOML & MSML

HR Services – HRXML

Business Services – ebXML

Web 2.0 Services – XML

Web Services – SOAP/XML

JEE Services – EJB/XML

.NET Services – COM/XML

IPTV Services – IPTV/XML

PDP

PMP

PCCP

PIP
Policy Orchestration for Control & Alignment
100+ POC, Pilot and Proto-types

- Ericsson, Nortel, 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