Key Enablers for the Cloud Service Broker: Identity, Privacy, and Security
OMG Telecom Cloud Workshop
Dec 6, 2010
David F. Chen
Lead Principal-Technical Architect
Ecosystem & Innovation, AT&T, Inc.
Agenda

• Introduction
• Evolution of Enterprise Cloud Computing Architecture
• Cloud Identity, Privacy, and Security – Challenges and Opportunities
• Cloud Services Brokerage
• Identity as a Service in the Telecom Cloud
The evolution of Enterprise Cloud architectures...

<table>
<thead>
<tr>
<th>Dedicated</th>
<th>Virtual</th>
<th>Utility</th>
<th>Cloud</th>
</tr>
</thead>
</table>
| Client #1
A
B
C
D
E
F
Client #2 |
| Client #1
A
B
C
D
E
F
Client #2 |
| A
B
C
D
E
F |
| Managed Hosting Services |
| Remote Infrastructure Management |
| Built to Order |
| Better Utilization |
| Dynamic Capacity |
| Self Service |
| Synaptic Hosting |
| Synaptic Compute as a Service |
How does Cloud differ from “Hosting” with Virtual Machines?

<table>
<thead>
<tr>
<th></th>
<th>Synaptic Compute as a Service</th>
<th>Synaptic Hosting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Servers (Guests)</td>
<td>Managed by Customer</td>
<td>Managed by AT&amp;T</td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Model</th>
<th>Self Service</th>
<th>Fully Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Interface</td>
<td>Portal, API</td>
<td>Support Team</td>
</tr>
<tr>
<td>Adaptability</td>
<td>Changes via API</td>
<td>Burstable</td>
</tr>
<tr>
<td>Billing Model</td>
<td>Hourly Consumption</td>
<td>Monthly Fee, Usage</td>
</tr>
<tr>
<td>Dedicated Hardware</td>
<td>n/a</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Example: Cloud Compute as a Service Options

Customers can select the number, size and type of virtual resources they need, and activate changes within minutes.

Virtual Guests

Resources
Billed Per Hour

<table>
<thead>
<tr>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 vCPU</td>
<td>2 vCPU</td>
<td>4 vCPU</td>
</tr>
<tr>
<td>4 GB RAM</td>
<td>8 GB RAM</td>
<td>16 GB RAM</td>
</tr>
</tbody>
</table>

Images

<table>
<thead>
<tr>
<th>Windows</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk space for each guest</td>
<td>File share across guests</td>
</tr>
</tbody>
</table>

Storage
Billed Per GB

Object storage accessible via REST API
Use Cases for Public/Private Clouds

**Disaster Recovery**
- Normal Traffic
- Cutover Traffic
- Data Copies
- Recovery Servers

**Server Bursting**
- Base Traffic
- Excess Demand
- Burst Traffic

**Live Application Migration**
- Continuous User Access
- Workload

**Global Workload Distribution**
- Private
- Public
- Users
- Workload
Some Use Cases for Storage as a Service

Internet Web Content
- Internet Web Content
- Web 2.0 Content, Media
- Intranet File Storage
- Employee Portals, Libraries, Collaboration

Long-Term Data Archival
- Corporate Network
- End Users
- Archive Manager

Intranet File Storage
- Corporate Network
- Employees

Short-Term Data Sharing
- VPN or Internet
- Third Parties

Slide 7 © 2010 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Enterprise Challenges

**Network**
- Secure private and public access
- Big bandwidth, low latency

**Security**
- Integrated, multilayer security model
- Intrusion detection, DDoS protection

**Performance**
- Globally consistent experience
- Optimization and acceleration

**Reliability**
- Fully redundant architectures
- Data center availability
Transforming How People Live and Work

Convergence of network, mobility, virtualization and cloud

Universal Access
Anywhere, Anytime
Any Device or Form Factor

Personal Persona
Business Persona

Network

Virtual Apps
Messaging
User Files
Content
Media

Opportunities

Virtualize the Infrastructure
Virtualize the End Points
Move Functionality to the Cloud
Manage the Apps & Content
Security Remains The No. 1 Barrier To Cloud Adoption Today

However, cloud security challenges will drive innovations and opportunities:

“Forrester fully expects to see the emergence of highly secure and trusted cloud services over the next five years, during which time cloud security will grow into a $1.5 billion market…”

- Jonathan Penn, Forrester Research, Inc.

“Cloud Services Brokerage (CSB) is the single largest revenue growth opportunity in Cloud Computing... CSB is Built on Markets Near 1 Trillion in Spend!”

- Daryl Plummer, Gartner
What is the greatest security risk to your cloud computing strategy? (from CSO Magazine)

- Ability to enforce provider security policies: 23%
- Inadequate training and IT auditing: 22%
- Access control at provider site: 14%
- Ability to recover data: 12%
- Ability to audit provider: 11%
- Proximity of company data to someone else's: 10%
- Continued existence of provider: 4%
- Provider regulatory compliance: 4%
Cloud Model

Security Control Model

- Applications
  - SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
- Information
  - DLP, CMF, Database Activity Monitoring, Encryption
- Management
  - GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- Network
  - NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- Trusted Computing
  - Hardware & Software RoT & API's
- Compute & Storage
  - Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
- Physical
  - Physical Plant Security, CCTV, Guards

Compliance Model

- PCI
  - Firewalls
  - Code Review
  - WAF
  - Encryption
  - Unique User IDs
  - Anti-Virus
  - Monitoring/IDS/IPS
  - Patch/Vulnerability Management
  - Physical Access Control
  - Two-Factor Authentication...

HIPAA
GLBA
SOX
Enterprise Business / Government Requirements
- a Shopping List

- Audits and Audit Trails
- eDiscovery
- Forensics Capability
- Policies and Procedures
- SAS70 (Type II)
- Card Processors – PCI (Certify Platform?)
- Health Data Processors (HIPAA, HITECH, etc)
- Privacy and Notification Laws (State and Fed)
- AntiVirus
- Risk Assessments, Pen-tests, Audits
  - Self Administered
  - 3rd Parties (PCI)
- Patch Management
- Firewalls
- Data Leak Protection
- Encryption Services
- Backup
- Monitoring Portals (Business Direct)
- Threat Management
- Data Destruction
- Physical Security
- European and other OCONUS Requirements

Data / Evidence should not just disappear when instance completes

For Govt, Add:
- NIST
- FISMA
- OMB
- GSA
- FIPS
- ITAR
- Etc.
Cloud Service Broker and Trusted Identity Broker

Benefits of Integrated “IDaaS”/“SaaS”:
- Trusted Identity
- Privacy
- Security
- Strong Authentication
- Identity Federation
- Fine-grained Authorization/Entitlement
- Compliance
- Risk Management
- Any time, any device
IDaaS Architecture Framework - A Telecom Cloud Enabler

- Security Token Service
- AuthN/AuthZ Service
- Entitlement Service
- Provisioning Service
- Federation Service
- GBA/GAA Service
- Key Management Service
- Role Mgmt Service
- Workflow Service
- Audit Service
- Compliant Service
- Risk Management
- Policy Management
- Identity Lifecycle Management
- Virtual Directory
- IDaaS Infrastructure
- Identity Repositories
- Policy Repositories
- Management & Admin
## CSA – IDaaS Common Recommendation

<table>
<thead>
<tr>
<th>Identity Mgmt Task</th>
<th>Consumer User</th>
<th>Corporate User</th>
<th>Web Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Access Control Model</td>
<td>RBAC, ACL</td>
<td>RBAC, ACL</td>
<td>ACL RBAC if requests on behalf of specific user</td>
</tr>
<tr>
<td>2a Authoritative Source – User Data</td>
<td>The user</td>
<td>The user’s organization</td>
<td>Varies depending on type of user and the web service client SPML or SAML</td>
</tr>
<tr>
<td></td>
<td>Local registration or OpenID</td>
<td>SPML or SAML</td>
<td></td>
</tr>
<tr>
<td>2b Authoritative Source – Policy Data</td>
<td>The cloud provider</td>
<td>The user’s organization</td>
<td>Information owner The cloud provider SPML or SAML</td>
</tr>
<tr>
<td></td>
<td>The cloud provider</td>
<td>SPML or SAML</td>
<td></td>
</tr>
<tr>
<td>3 Privacy Policy</td>
<td>The cloud provider Implement locally</td>
<td>The user’s organization XSPA profile for XACML</td>
<td>Client organization XSPA profile for XACML</td>
</tr>
<tr>
<td>4 Access Control Policy Format</td>
<td>XACML</td>
<td>XACML</td>
<td>XACML</td>
</tr>
<tr>
<td>5 Policy Transmission</td>
<td>N/A</td>
<td>SPML or SAML 2.0 profile of XACML</td>
<td>SPML or SAML 2.0 profile of XACML</td>
</tr>
<tr>
<td>6 User Profile Transmission</td>
<td>OAuth</td>
<td>SAML assertion</td>
<td>SAML assertion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OAuth</td>
<td></td>
</tr>
<tr>
<td>7 Policy Decision Request</td>
<td>N/A</td>
<td>XACML, SAML2.0 profile of XACML</td>
<td>XACML, SAML2.0 profile of XACML</td>
</tr>
<tr>
<td>8 Policy Decision Enforcement</td>
<td>Do within application Locally specified ACLs for non-corporate entities OAuth to share with other sites</td>
<td>Do within application XACML for policy specification from PAP OAuth to share with other sites</td>
<td>Do within application or externalize to web service gateway product.</td>
</tr>
<tr>
<td>9 Audit Logs</td>
<td>Log activity –</td>
<td>Log activity – encrypt with</td>
<td>Log activity – encrypt with time stamp</td>
</tr>
<tr>
<td></td>
<td>encrypt with time stamp</td>
<td>time stamp</td>
<td>with time stamp</td>
</tr>
</tbody>
</table>
IDaaS Standard and Solution Requirements

• SPML 2.0, SAML 2.0, OAuth 2.0, XACML 2.0/3.0, WS-Trust: Security Token Service (STS)
  • OAuth 2.0 adds new Authorization Server component, which can be a combination of XACML and STS services for providing RESTful based service to service authorization and user privacy consent management architecture framework.

• GBA/GAA, OATH (OTP), and other multi-factor authentication solutions

• OpenID – mainly for consumer customers

• Information Cards

• Identity Assurance and OIX (Open Identity Exchange) Trust Frameworks
Roles of GBA in Telecom IDaaS

• 3GPP GBA (Generic Bootstrapping Architecture) is a mechanism to bootstrap authentication and key agreement for HTTP based application security from the 3GPP AKA (Authentication and Key Agreement) mechanism.

• GBA can be easily integrated with multiple web based identity standards, e.g. OpenID, SAML, and InfoCards etc.

• GBA enables telecom service providers to be a trusted identity provider with strong authentication (bootstrap + user PIN) and enhanced user experience (user doesn’t need to enter password in mobile phone!).

• 4G Americas IdM project I chaired and it’s paper [here](#) introduced a reference architecture for enabling a telecom provider as IdP by integrating GBA with web based identity standards such as OpenID, SAML, XACML, and InfoCards etc.
Customers use IDaaS as an Identity Broker to access their cloud and on-premise services using their enterprise identities.

- **Enterprise Customer**
  - IdM
  - Directories
  - Enterprise IdM

- **End User** (Employee, customer, partner)
  - Validates user ID/Password

- **Telecom IDaaS**
  - Validates OTP or Mobile Signature
  - SSO with cloud services and on-premise applications

- **Public Cloud Services**
  - Allows access
  - Accesses protected service which requires OTP for two-factor authentication or Mobile Signature

- **Private Cloud Services**
  - Validates user security token

- **Community Cloud Services**

**Provides value-added IdM services:**
- GBA and OTP two-factor based Strong Authentication Service
- Mobile Signature service
- Federation Service
- Identity Assurance
- Policy-based Authorization