Kantara Initiative Workshop

Identity as Security Glue for the Cloud

Matthew Gardiner
CA Inc.

&

Chris Sharp
MEDecision
Identity is Central to Cloud Security & Management
The Cloud Hype is at Fever Pitch

Last year we recognized that our processes were far too complex.

So we put them into the cloud.

Let the clouds make your life easier.
Agenda

Identity as Security Glue

Health Services From the Cloud

Takeaways
What is the Cloud?

- SaaS
- PaaS
- IaaS
- Private Cloud
- Public Cloud
- Hybrid Cloud
Cloud Model Drives Security Implications
Identity as Security Glue - Points of View

1. Extend Enterprise Security to Cloud Services [Enterprise to Cloud Providers]
   - Examples…User provisioning to Cloud, Federated SSO to Cloud, Log collection pulling from Cloud to enterprise

2. Enable Cloud Providers to better secure their services [For Cloud Providers]
   - Examples….Controlling the privileged user in the Cloud, Administering the entitlements of all classes of users, Controlling access to Web applications & services in the Cloud, Federating user sessions to other Cloud providers

3. Enable Cloud Providers to offer Security/IAM services to organizations [Cloud Providers for Enterprise]
   - Examples….Authentication service from the Cloud, Log management service from the Cloud, DLP service from the Cloud
## Identity as Security Glue - Mapping Identity Services to Cloud

<table>
<thead>
<tr>
<th>Identity Services</th>
<th>Points of View</th>
<th>Enterprise To Cloud Providers</th>
<th>For Cloud Providers</th>
<th>Cloud Providers For Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged User Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Leak Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Provisioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Authentication &amp; Federation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Access Management/SSO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Services Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Identity as Security Glue - Areas of Relevance

<table>
<thead>
<tr>
<th>Points of View</th>
<th>Enterprise To Cloud Providers</th>
<th>For Cloud Providers</th>
<th>Cloud Providers For Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged User Management</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Data Leak Protection</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>User Provisioning</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Role Management</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>User Authentication &amp; Federation</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Web Access Management/SSO</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Web Services Security</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Log Management</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
</tbody>
</table>
# Identity as Security Glue - Most Immediate Need

<table>
<thead>
<tr>
<th>Identity Services</th>
<th>Points of View</th>
<th>Enterprise To Cloud Providers</th>
<th>For Cloud Providers</th>
<th>Cloud Providers For Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged User Management</td>
<td></td>
<td></td>
<td>⭐️</td>
<td></td>
</tr>
<tr>
<td>Data Leak Protection</td>
<td></td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
</tr>
<tr>
<td>User Provisioning</td>
<td></td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Authentication &amp; Federation</td>
<td></td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
</tr>
<tr>
<td>Web Access Management/SSO</td>
<td></td>
<td></td>
<td>⭐️</td>
<td></td>
</tr>
<tr>
<td>Web Services Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Management</td>
<td></td>
<td></td>
<td>⭐️</td>
<td>⭐️</td>
</tr>
</tbody>
</table>
Health Services From the Cloud
Secure access to Healthcare data

Applications
- Web portal
- Electronic medical record
- Practice management system
- Picture archiving & comm systems
- Personal health record
- Care management system
- Utilization management system
- Disease management system

Data
- Clinical
- Administrative
- Financial

Knowledge
- Gaps in care
- Potential errors
- Alerts/Notifications

Analytics

Provider
- Demographics
- Lab results
- Imaging results
- Medical summaries
- Scanned documents

Payer
- Demographics
- Claims

Ancillary
- Demographics
- Lab results
- Imaging results

PHR
- Demographics
- HRAs

PBM / Pharmacy
- Demographics
- Medication history

Public Health
- Demographics
- Immunizations
Creating a service-enabled environment

Service-enabled environment

Exposed Partner Web Service

Web Service Consumer
CCR Engine

Exposed Partner Web Service
WSDL
CCR XSD Schema

Aggregation Services
Get Member Data
Get Clinical Data

Services
Validate Member ID
Get Member Address data
Get Treatment data

Resource Adapters
LDAP
DB2
Oracle (Hibernate)

Internet

Image of network topology and data flow.
Access based on partner entitlement

– Certificates on a Web server were a good start but…
  • It does not easily allow for role-base access
– Implementation of role-based access to web services allows for:
  • Secure Web services using partner certificates
  • Identify partners based on the digital signature
  • Apply additional role-based access rules
  • Encrypt/Decrypt the message
– We chose to use WS-Security because of the partners we’re dealing with
– Change to other authentication schemes (like SAML) is simply a change in configuration
Applying authorization rules

Questions:
- Who is the partner?
- What web service are they calling?
- For what health plan?
Applying role-based access

Policy 1

Web Service: SummaryView  
HealthPlan: HealthPlanA

Policy 2

Web Service: DetailView  
HealthPlan: HealthPlanA

Policy 3

Web Service: DetailView  
HealthPlan: HealthPlanB

Partner A

Access to Summary view and Detail view for HealthPlanA

Partner B

Access to Detail view for HealthPlanA and HealthPlanB
Combining SAML and web services

User

Internet

SAML Assertion

iEXCHANGE Web

Federation Manager

Allow access

SSO Web Service

Plan portal

Authenticate Here

Security Product

Is the group mapped?
Takeaways
Takeaways

• Identity is key security glue for the cloud

• Federation standards are central
  – SAML, WS-Security, OpenID, IMI, XACML, SPML….
  – Fortunately the security industry foresaw the cloud
  – But we must recognize new players need to be educated

• Challenges remain the same
  – Privacy, liability, contracts, economics, interoperability…

• Harness the “cloud hype” to continue to progress our identity mission