Corporate Identity Considerations for Cloud and ASP Application Vendors

Joe Bate
Senior Security Architect
Disclaimer

- The points of view or opinions contained within this document are those of the author and do not necessarily represent the official view, position or policies of his employer.
- Diagrams provided are for discussion purposes and not technically accurate. Each of the processes and flows have an infinite number or variations.
Background

■ What is Cloud Computing?
  ● Common
  ● Location Independent
  ● Online
  ● Utility
  ● On-Demand

■ What is an ASP Application?
  ● A computer based service on the network
  ● May or not be multi-tenant

■ What is a Cloud Application?
  ● ASP application hosted in a Cloud
  ● Multi-tenant
  ● a.k.a. Software As A Service (SaaS)
Key Areas of Consideration in Corporate Identity Management

- **Provisioning**
  - Centralized management of user identity information, accounts and attributes.
  - May involve the creation, modification, deletion, suspension, restoration of a defined set or accounts, privileges and/or attributes.
  - May involve the execution of a defined business or system process.

- **Attestation**
  - Validation the access the user has been granted is what they should have for their role in the organization

- **Exceptions for Remediation**
  - Delta between what access the user has been granted and actually have

- **Entitlement and Attestation**
  - Entitlement
    - What access the user has been granted

- **Access Control**
  - Authentication
    - Single Sign On
    - Identity Assurance
  - Authorization
Traditional – Use Case Model
Traditional - Sign-On

Requires additional tools such as ESSO for Single Sign-On

Corporate Identity Considerations for Cloud and ASP Application Vendors
Traditional - Provisioning

Corporate Identity Considerations for Cloud and ASP Application Vendors
Traditional – Entitlement and Attestation Reporting

Often manual process
Traditional Approach

Identity Administrator

Internal Authentication System

Identity Repositories

End User

Application Administrator

Service Provider Application

Entitlement Manager

Hiring Manager

Resource Owner

Corporate Identity Considerations for Cloud and ASP Application Vendors
Issues with the Traditional Approach

- Usernames and Passwords present the following challenges:
  - **Cost:**
    - Helpdesk calls for resets on infrequently used password
  - **Risk:**
    - Poor password handling, as user often write down the password
    - Weak password, so they are easy to remember
    - Reuse of passwords between internal and external systems, often creating an external weakest link
    - Password disclosure through credential sharing or social engineering

- Password complexity and strength is limited to remote system and the end user

- In many cases user may access Internet ASP application external from corporate premises or assets.
  - This can lead to unauthorized use of resources, such as terminated employee still retaining access after leaving organization.

- Loss of productivity of business users due to time delays in accessing systems as the lookup or attempt to remember or have to have password reset.

- Delays in the suspension or termination of accounts can result in unauthorized access to systems and data.
Issues with the Traditional Approach

“The dark ages before Identity Management”*

- Isolated directories and databases containing same information about people within and external to the company
- Every application has own user management and every additional application compounds the problem
- Linkage of accounts and users becomes extremely hard to manage
- Redundancy of data and administration means high costs
- Process for provisioning accounts very slow
- User often get access to resource to late
- Even worse user keeps access after leaving the job
- There’s no real security in chaos

* Unknown author
Industry Trends

- Trending towards more outsourcing technology through use of Cloud and ASP Applications, this will become more prevalent once Privacy, Data Residency and Security concerns are overcome.
- As the number of web applications increases, users are having to set up with more and more online digital identities, driving changes to the way Corporation need to handle their user identities.
- Regulatory compliance is driving better protection user security and privacy, through careful management of user identities, throughout their life cycles from creation to termination.
- Advances in IdM Industry Standardization and Alignment
- Advances IdM Technology/Industry Interoperability
Industry Standardization

Main SSO Technologies:
- SAML
- OpenID
- InfoCard

Web Application Targeted

Industry groups
- specifications
- encourage use

Main attribute exchange technology
- ID-WSF

* Standardization Trends in Identity Management Technologies
Industry Alignment

<table>
<thead>
<tr>
<th>Authentication Federation Schemas</th>
<th>Attribute Exchange Schemas</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML v2.0</td>
<td>ID-SIS</td>
</tr>
<tr>
<td>Regulates authentication federation and account linking schemas</td>
<td>Regulates schemas for the declaration of attribute information</td>
</tr>
<tr>
<td>• Single sign-on</td>
<td>• Personal profiles, employee profiles</td>
</tr>
<tr>
<td>• Single logout</td>
<td>• Geolocational data, calendar services, etc.</td>
</tr>
<tr>
<td>• Account federation</td>
<td>People Service</td>
</tr>
<tr>
<td>• Others</td>
<td>Regulates schemas for sharing user attributes between web services</td>
</tr>
<tr>
<td></td>
<td>• User attribute manager search scheme</td>
</tr>
<tr>
<td></td>
<td>• Attribute data request/response schemas, etc.</td>
</tr>
<tr>
<td>ID-WSF v2.0</td>
<td>Advanced Client</td>
</tr>
<tr>
<td>Regulates schemas for sharing user identities to terminals</td>
<td></td>
</tr>
</tbody>
</table>

Existing specifications used for communication schemes and security specifications (XML, XML dSig, XML Enc, SOAP, WS-* etc., etc.)

* Standardization Trends in Identity Management Technologies

Liberty Alliance ID FF has developed into SAML v2.0, which is now regulated by (OASIS).

SAML v2.0 is also referenced by ITU-T. In the form of Recommendation X.1141

Limited SAML 2.0 supported with release of Microsoft Geneva (ADFS)
### Telecom Industry

<table>
<thead>
<tr>
<th>Recommendation No.</th>
<th>Recommendation name</th>
<th>Scheduled agreement date</th>
<th>Editor (affiliation &amp; country)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y.2720</td>
<td>NGN identity management framework</td>
<td>Approved (Jan. 2009)</td>
<td>Richard Brackney (DoD, USA), Takashi Egawa (NEC, Japan)</td>
</tr>
<tr>
<td>Y.NGN IdM Requirements (draft)</td>
<td>NGN identity management requirements</td>
<td>May 2009</td>
<td>Martin Dolly (AT&amp;T, USA), Enhui Liu (Huawei, China), Anthony Rutkowski (Verisign, USA), Ray Singh (Telcordia, USA)</td>
</tr>
<tr>
<td>Y.NGN IdM Mechanisms (draft)</td>
<td>NGN identity management mechanisms</td>
<td>Sep. 2009</td>
<td>Takashi Egawa (NEC, Japan), Zachary Zeltsan (Alcatel-Lucent, USA)</td>
</tr>
<tr>
<td>Y.NGN IdM Use-cases (Technical Report) (draft)</td>
<td>NGN identity management use cases</td>
<td>May 2009</td>
<td>Martin Dolly (AT&amp;T, USA), Paul Knight (Nortel, USA), Ray Singh (Telcordia, USA)</td>
</tr>
</tbody>
</table>

### Standardization Trends in Identity Management Technologies

- **Q16/13** which is investigating security and IdM in future networks including Next Generation Networks (NGNs)

- Jan 2009 Y.2720 was approved by ITU-T as first stage of recommendations

- **Q10/17** which is investigating IdM architectures and security mechanisms.

* Corporate Identity Considerations for Cloud and ASP Application Vendors*
Industry Interoperability

* Standardization Trends in Identity Management Technologies

Corporate Identity Considerations for Cloud and ASP Application Vendors
Federation - Use Case Model

Corporate Identity Considerations for Cloud and ASP Application Vendors
Federation - Sign-On

Example Based on Fully Trust Model

Corporate Identity Considerations for Cloud and ASP Application Vendors
If persistent tokens are used, the Application Admin/System may also be required to push data to the Service Provider either through traditional or other methods such as SPML automation.
Federation – Entitlement and Attestation

If persistent tokens are used, Application Admin/System must also pull data from Service Provider and due Exception handling.
Federation
Authorization @ Consumer
Corporate Identity Considerations for Cloud and ASP Application Vendors

Federation
Authorization @ Service Provider

Identity Administrator

No Always Required / Alternatively can be captured from Token Attributes

End User

Secure Token Service/Exchange

Internal Authentication System

Identification Repositories

Hiring Manager
Resource Owner

Corporate Identity Considerations for Cloud and ASP Application Vendors

Application Administrator

Service Provider Application

Entitlement Manager
Cloud and ASP Application Design Considerations

- Applications should be designed with externalized Identity Management in mind
  - Removing silo Identity Management from the application should allow changes to occur without application design impact.
  - Expect SAML 2.0 to be the Token of preference for the next few years
  - Expect SAML HTTP Post to be preference over Artifact Resolution
  - Avoid the use of persistent tokens where possible

- Applications should be designed using role based access control
  - Design application role complexity should be at service consumer discretion where possible

- Applications should be designed expecting minimal user attributes

- Applications should be designed expecting that they will no longer have or require a local user repository

- Applications should be designed expecting an increasing demand for a usage based licensing model

- Applications should always be designed with Privacy, Data Residency and Security in mind.
References and Useful Links

- [https://www.ntt-review.jp/](https://www.ntt-review.jp/) - NTT Technical Review
  - Standardization Activities of the Liberty Alliance
  - Standardization Trends in Identity Management Technologies
  - Recent NGN Security Standardization Trends
- [http://informationcard.net/](http://informationcard.net/) - The Information Card Ecosystem
  - [EAuthFederationArchitectureInterfaceSpec](http://www.cio.gov/)
  - The Venn of identity
- [http://www.ipc.on.ca/](http://www.ipc.on.ca/) - Office of the Information and Privacy Commissioner/Ontario