Linking Services and Data in the Cloud

Martin Bauer, Amardeo Sarma
NEC Laboratories Europe
If you search for “linked data” and “cloud”, you first find this:

Publish data as Linked Data:
(i) assign consistent URIs to data items
(ii) generate links
(iii) publish metadata which facilitates further exploration and discovery of relevant datasets.


... in this talk we rather look at cloud computing, the user, and how to link the two, and then try to find out how this relates to “linked data”
We will have a mix for some time

- Services appear in the cloud
  - Sales, CRM, calendar, email, …

- Enterprises and homes still run local services
  - Some things are preferred as local services
  - Intranet services, WLAN likely to remain local

- Operator services already used today
  - Mobile phone, hotspot, home gateway, …

- Future solutions must allow an arbitrary mix of local, operator & cloud services
Identity is the choice to bridge worlds in the cloud
A future typical mix

In-House
- Financial
- HR
- CRM

Cloud
- Data storage
- CRM e.g. Salesforce

Hosted or Managed
- Web Presence
- Mail e.g. Exchange
- Workflow

Telco
- Mobile Phone
- Shopping
- Hot spot access

Migration
Identity
Linking data and services via identities

User Addition / Removal
SSO Environment
User Profile Sharing
Consistent Access Control

HR Data
Sales Data
SAP
DB
CRM
Identities
Local Service
Local Data
CRM Data
Scenario: Linking (mashing up) data from two providers

- User wants to create a Leaflet
  - using an online leaflet creation tool
  - using photo from a photo library

- User has different roles
  - Private
  - Work-related
  - Member of a club

- Roles can be represented using different identities

- Different access rules can apply for different identities, i.e., different pictures can be used when authentication with private, work-related and club-related identity.
Underlying actions for realizing scenario

Unified Authentication

Distributed Access Management

Secure Mash-Up Usage

Access is linked via common (virtual) identity
Virtual identity

- Creation of different profiles
- Association of different attributes
- Selection of profiles for:
  - Authentication
  - Exchange of attributes
- Protection of privacy:
  - Identity
  - Attributes
- Distributed Attributes possible
Single sign-on despite different protocols

Welcome to the IdBroker,
you may now sign in to your account.

You are trying to access [http://localhost:8081/np].

Name: john.swift
Password: ********

Keep me signed in.
Login | Cancel request

Forget your login information?

Login (SSO)
Please enter your OpenID!
http://www.my-idp.demo:808

Login
Please enter your user name and password
Username
Password
Login

Single Sign-On
For SSO, please choose
< your SAML provider > Login

This site supports single sign-on.

SAAML
Overall summary of scenario

- Enterprises has outsourced some services into the cloud, but still wants to keep some control.

- Employee uses editing a leaflet and needs image for illustration.
  - Authentication with different protocols (SAML, OpenID).

- Pool of available images is limited through local and enterprise policies.
  - Distributed Access Control.
Key issues to solve

General challenges

Making data and services accessible to users
- However protecting unauthorized access
- Catering for different roles of the users
- Linking or mashing up data and services as needed

Allowing migration of data and services
- From protected areas into the cloud
- Within the cloud across providers

Protecting data and services in the cloud
Relation to Linked Data and what is within scope?

- If we represent information as linked data, what does that mean for the user and his/her identity?
- How do we identify the user?
- How do we deal with different roles?
- How is access to user information protected?
- Different aspects should NOT be directly linkable – but there are situations in which you may want to link (e.g. emergencies) – so it may depend on who is asking and in what situation
- Does Linked Data consider “indirect linking”?
- Can we have a trusted entity that has the linking information and can allow it in special cases?
- Or is this all outside the scope of Linked Data?