Identity 2.0 and User-Centric Identity

Dr. Oliver Pfaff, Siemens AG
ZKI AK Verzeichnisdienste, Berlin 2008-03-10
Setting the Scene
Presentation Goals

- This presentation discusses new concepts, patterns and technologies emerging around the notions of “Identity 2.0” and “User-Centric Identity”:
  - It emphasizes their relationship with directory systems (Identity 2.0 = Directory 2.0?)
  - It presents a vendor’s view upon these initiatives
  - It not meant to be a product marketing presentation
Agenda

- **Identity 2.0**
  *What Is Changing and Why?*

- **Web Services**
  *How Do They Change the Landscape?*

- **User-Centric Identity**
  *How Does It Work?*

- **Example: eFA**
  *How Does It Classify?*

- **Conclusions**
Identity 2.0

Assets and Liabilities

Traditional approach: *piggybacked*

- **Service**
  - **Authz subsystem**
    - Consumes
    - **Authn subject:**
      - `id=John Doe`
      - `cakePref=Streusel`
      - `authnMethod=SSL`
    - Produces
      - **Initial authn endpoint**

- **Initial authn protocol**
  - Cert=MI...
  - PoP=SSLSign(SrvNonce)

- 🙁 Causes identity enclaves
- 🙁 Mandates RPs to be IdPs
- 😞 ...

Federated approach: *split work*

- **Service**
  - **Authz subsystem**
    - Consumes
    - **Authn subject:**
      - `id=John Doe`
      - `cakePref=Streusel`
      - `authnMethod=SSL`
    - Produces
      - **Fed. authn endpoint**

- **Fed. authn protocol**
  - Assertion=<id=John Doe, prefCake=Streusel>
  - PoP=WSSESign(SrvNonce)

- User account:
  - `id=John Doe`
  - `altSubjectId=MI...
  - `cakePref=Streusel`

- Attr mapping:
  - `prefCake::= cakePref`

Copyright © Siemens AG 2008 All Rights Reserved
Identity 2.0
The Missing Link: Beaming Authentication

Identity provider

Transient, authenticated subject data

Away

Federated authentication

Home

Resource provider

Persisted, unauthenticated user data

Initial authentication

Start

Identity provider

Initial authentication

Initial authentication

Initial authentication

Provisioning

Identity provider

User data

User data

User data

Identity 1.0 pattern options:

Identity 2.0 pattern:
Identity 2.0

...Is Being Resolved Now

- Use case: want to authorize resource access requests
  - without being obliged to maintain user accounts for everybody in the user population i.e.
  - without being able to initially authenticate every user

- Requirements:
  - Maximal resource and identity provider decoupling
  - User and privacy-friendliness: ease-of-use, user empowerment, self-determination…
  - Security
Identity 2.0
On the Evolution of Identity

Perception of identity

Transient, authenticated subject data

Persisted, unauthenticated user data

Local matter

Transient, authenticated subject data

Persisted, unauthenticated user data

Local matter

Transient, authenticated subject data

Persisted, unauthenticated user data

Joint matter

Transient, authenticated subject data

Persisted, unauthenticated user data

N.a.

Perception of identity

Transient, authenticated subject data

Persisted, unauthenticated user data

N.a.
Web Services

Needs Shared With Web Applications

- Traditional Web application environments (HTTP/HTML) and Web services (HTTP/SOAP) share needs regarding an Identity 2.0 support:
  - Express authenticated subject information and related meta-data
  - Support multiple concepts for identifier abstractions
  - Support arbitrary subject attributes (to decouple consumers from a need to perform look-ups)
  - Support a variety of authentication schemes (to obtain a statement on authenticated subject identity, to protect such statements and bind them to subjects)
- SAML assertions provide the best-practice approach to address these shared needs. They are used in Identity 2.0-enabling traditional Web application environments as well as Web services.
Web Services
Deviations from Web Applications

- The tricky part is the acquisition and exchange of SAML assertions:
  - How to tell that there is a need to present a SAML assertion
  - How to express expectations on SAML assertion issuer and contained information
- Traditional Web application environments and Web services differ significantly:
  - Web applications:
    - Tedious to design and realize the piggybacking of SAML assertions and their acquisition/exchange protocol with HTTP/HTML-based communications
    - Several approaches emerged over time:
      - First generation:
        - First wave (2001-2003): SAML 1.x, Shibboleth, Liberty-Alliance
        - Second wave (2004-2005): SAML 2.0, WS-Federation (for passive requestors)
      - Second generation (2006):
        - Microsoft CardSpace (for passive requestors), OpenID
  - Web services:
    - Simple to design and realize the piggybacking of SAML assertions and their acquisition/exchange protocol with HTTP/SOAP-based communications
Web Services

Architectural Abstractions

- Following standard Web services concepts and components support the Identity 2.0-enabling of Web services:
  - Request SAML assertions
    - Require e.g. ProtectionToken in WS-SecurityPolicy section in WSDL. This also allows to specify the expected properties (attributes, claims) of SAML assertions which need to be presented and the protection scheme for them (PoP)
    - There is no equivalent concept for traditional Web application environments (requires specifically designed vocabulary transferred with HTTP messages)
  - Issue SAML assertions
    - Addressed by WS-Trust STSs as a dedicated service for SAML assertion issuance (notes: SAML assertions can also be issued by non-STSSs; STSs can also issue non-SAML assertions)
    - There is no equivalent concept for traditional Web application environments
  - Transfer SAML assertions
    - Addressed by the SAML token profile in WSSE
    - There is no equivalent concept for traditional Web application environments (embedding of SAML assertions is outside HTTP headers)
### About WS-Trust

- **WS-Trust** is a key concept in WS-security that deals with authentication diversity:
  - Different systems have different authentication needs and prefer different techniques to prove or verify claimed identity
  - Using the same credential for everything is not secure and not practical.
- Abstracts from specific means of authentication by introducing security tokens as an umbrella concept for artifacts that are ubiquitous in authentication systems
  - Security token examples: X.509 certificates, Kerberos tickets, SAML assertions…
- Defines a framework for processing security tokens (issuance, renewal, cancellation, validation, negotiation)
  - A WS-Trust STS (Security Token Service) is a Web service that processes security tokens
Facilitate user-centric identity

Examples:
- SAML Web-SSO
- Shibboleth
- Liberty-Alliance ID-FF
- WS-Federation

Example: OpenID

User-Centric Identity
Types of Identity 2.0 Solutions

Transparent to users

Federated authentication

Information card-based
Example: CardSpace

Facilitate user-centric identity

Identifier-based
Example: OpenID
User-Centric Identity
What Is OpenID?

- OpenID is a decentralized, open-source framework for user-centric digital identity
  - Identity perception: transient, authenticated subject data
- Based on following concept:
  - Users have network authentication services dedicated to them individually (e.g. johndoe.myopenid.com)
  - URLs of these authentication services serve to claim an identity (I am johndoe.myopenid.com)
  - Transfer of authenticated information to RP from IdP is subject to user approval
- More information: http://openid.net/
User-Centric Identity
Brief OpenID Assessment

- What’s new – one thing is cool in OpenID:
  - OpenID introduces network authentication services that are dedicated to individuals
    - Lifts the joint identity perception from persisted, unauthenticated user data to transient, authenticated subject information
    - Provides means for individuals to control the sharing of personal information and establishment of relationships with other parties at the authentication service

- What strikes – several things are over-simplified in OpenID:
  - From a structural perspective, OpenID resembles a SAML post profile exchange but OpenID replaces structured data that is expressed in XML in traditional federation protocols by ad-hoc encodings directly transferred as keyword/string value-pairs
  - Keying association establishment avoids PKI concepts and uses anonymous Diffie-Hellman for an ad-hoc association establishment. This exposes OpenID systems to impersonation and man-in-the-middle attacks.
User-Centric Identity

What Is Windows CardSpace?

- CardSpace is a Microsoft client application helping users to manage and use their digital identities.
  - Identity perception: transient, authenticated subject data
- Provides a part of novel user authentication and identity federation systems; represents their identity selector artifact.
- Is a milestone towards an identity metasystem:
  - An identity metasystem integrates islands of identity with their “local” identity technologies
  - Analogy: IP provides a communication metasystem for integrating islands of LANs with their “local” communication technologies.
- Allows arbitrary parties to become resource and identity providers
- Is standards-based
User-Centric Identity

Windows CardSpace: Fundamental to Differentiate

- Identity metadata: templates for identity data plus references to identity providers
  - *E.g. Authenticated subjects will be represented by RFC 822 name, organizational affiliation and role values; actual data can be obtained at these endpoints*…
  - Consists of attributes without their values e.g. `name, affiliation, roles`
  - Represented as long-lived objects called information cards in CardSpace
  - Sample:

```
<XML Document
```

- Identity data: concrete information about authenticated subjects
  - *E.g. This is ‘John Doe’, an employee of ‘Acme’ with the role ‘manager’*
  - Consists of attributes with their authenticated values e.g.
    - `name=John.Doe@Wipro.example, affiliation=Wipro, roles=Manager`
  - Represented as short-lived objects called security tokens in CardSpace (aka: transient, authenticated subject data)
  - Sample:

```
<XML Document
```
User-Centric Identity
CardSpace High-Level Architecture

1. Security policy

User agent

Identity selector
(consumes identity metadata)

2. Information card selection

Identity provider
(produces identity data and identity metadata)

Resource provider
(consumes identity data)

0. Information card

3. Security token

Identity metadata sharing
User-Centric Identity

CardSpace Highlights

- Not “Passport 2.0”
- Not limited to deployments in federated environments. CardSpace can also be used for user authentication within an enterprise.
- Resembles design elements of traditional identity federation approaches:
  - Structured data is represented in standard XML representations (SAML, WS-*)
  - Keying associations are based on PKI concepts
- But provides several advances over them:
  - Identity metadata sharing between identity providers and users
    - Improves identity and resource provider decoupling
    - Facilitates user-centric identity and supports users in controlling the proliferation of personal information
    - Improves user guidance through login procedures
  - Process isolation for the identity selector lifts host-security to a new level (anti-malware / phishing / pharming features)
  - Web services security employment resolves HTTP/HTML security restrictions
- Note that CardSpace is part of a larger identity metasystem initiative (cf. www.identityblog.com) at Microsoft.
eFA
Project Characteristics

- A national project to introduce federation in accessing patients’ MDOs
  - According medical cases
  - Across health providers
- Project goal: specify and pilot a solution architecture
- Project participants:
  - German hospitals (project owner, solution users) incl. Rhön Klinikum AG
  - Suppliers of IT solutions (technical realization) incl. Siemens Med
  - Fraunhofer ISST (specification lead)
- Piloting will done between pairs of recognized hospitals which each have an industry partner for the technical realization. In case of Siemens Med:
  - Universitätsklinikum Giessen (www.uniklinikum-giessen.de) belonging to Rhön Klinikum AG with the industry partner Siemens Med
  - Kreiskrankenhaus Lich (www.askaepios.com/Lich) belonging to Asklepius with the industry partner Microsoft
- More information: www.fallakte.de
ECRs (Electronic Case Records) provide structured and integrated views of MDOs related to a single medical case:

- They contain MDOs by reference
- Location of contained MDOs can span across various health providers
- They represent a physician's tool for cooperation with other physicians in order to treat diseases.
- They aim at adding value beyond individual MDOs, not at interfering or reinventing MDOs
## eFA Architectural Approach (v0.16 WSDLs/XSDs)

<table>
<thead>
<tr>
<th>Web service clients</th>
<th>Web services</th>
<th>Data objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityProvider STS client</td>
<td>authenticate, ...</td>
<td>IdentityProvider STS</td>
</tr>
<tr>
<td>AttributeProvider STS client</td>
<td>getAttributes</td>
<td>AttributeService STS</td>
</tr>
<tr>
<td>ECRAdmissionToken Provider client</td>
<td>requestAdmissionToken Collection, ...</td>
<td>ECRAdmissionTokenProvider</td>
</tr>
<tr>
<td>ECRRecordRegistry Security client</td>
<td>requestAccess, ...</td>
<td>ECRRecordRegistrySecurity</td>
</tr>
<tr>
<td>ECRRecordRegistry client</td>
<td>getFolderList, ...</td>
<td>ECRRecordRegistry</td>
</tr>
<tr>
<td>ECRDocument Registry client</td>
<td>getInformationObject List, ...</td>
<td>ECRDocumentRegistry</td>
</tr>
<tr>
<td>ECRDocument Repository client</td>
<td>getInformationObject, ...</td>
<td>ECRDocumentRepository</td>
</tr>
</tbody>
</table>

*Attrs esp. role, memberOf*
Conclusions

- Identity 2.0 and user-centric identity will change the identity management agenda:
  - Identity 2.0 shifts the perception of user identity from persisted, unauthenticated data to transient, authenticated information. It is a reaction for limitations of traditional security architectures with their rigid coupling between authorization and authentication.
  - User-centric identity puts self-determination of individual users into the identity management focus. It is a re-percussion to Web 2.0 approaches around user participation.

- Web services change the technology landscape. They especially simplify federation. Federation solutions for traditional Web application environments and Web services should be regarded as different generations.

- A short taxonomy of federation solutions with the dimensions of Web services / Identity 2.0 / user-centric identity:

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Identity 2.0</th>
<th>User-centric</th>
<th>Web service-aware</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Web-SSO, Shibboleth, Liberty-Alliance ID-FF</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>OpenID</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CardSpace</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>eFA</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Backup
Laws of Identity
(Source: Kim Cameron, Microsoft)

- User control and consent
- Minimal disclosure for a defined use
- Justifiable parties
- Directional identity
- Pluralism of operators and technologies
- Human integration
- Consistent experience across contexts

Join the discussion at www.identityblog.com
User-Centric Identity
CardSpace Sequence Diagram (for Web Browsers)

**User**
- Access any resource

**User agent**
- GET any RP resource
- Redirect to RP login page
- GET to RP login page
- (with HTML tag representing the RP security token policy)
- GetBrowserToken(RP policy)

**Identity selector**
- Provide information card (out-of-band)
- WS-MEX GetMetadata Request
- WS-MEX GetMetadata Response
- WS-Trust RST Request (user credentials)
- WS-Trust RSTR Response (security token)
- Return security token
- POST to RP FEP (with security token)
- Redirect to any resource (with RP session cookie)
- GET any RP resource (with RP session cookie)
- Response any resource

**RP**
- Authz

**IdP**
- Initial authn

- HTTP/HTML-defined
- WS-* defined
- SAML-defined
- SAML-defined

Copyright © Siemens AG 2008 All Rights Reserved
Identity 2.0

The Traditional System Architecture Pattern

User

User agent

Identity provider (produces authn identity, consumes user data)

Resource provider (consumes authn identity)

Has: user identifier, credential

Persisted data, in brain...

Claimed user identifier, credential

Authenticated user identifier, attributes

Transient data, in memory

Initial authn

Persisted data, in repository

Tight coupling

Has: user accounts = user identifiers, attributes, credentials

Copyright © Siemens AG 2008 All Rights Reserved
Identity 2.0

...Is Limited

- Characteristics:
  - Bundles authorization and initial authentication through a tight coupling
  - Produces authenticated subjects from persisted data only – via own initial authentication
  - Supports externalization on a persistence level only

- Limitations:
  - Lacking separation of concerns:
    - Mandates resource providers (short: RP) to accommodate identity provider (short: IdP) tasks
  - Missing wide-area capabilities of identity:
    - Authenticated subject identity can not be transferred
    - Remedies within the traditional pattern ... don’t solve the problem:
      - Transfer persisted user data:
        - Requires to re-do initial authentication again and again – the SSO problem
        - Violates the “better refer than copy” principle in IT
      - Refer to persisted user data from external sources:
        - Requires to re-do initial authentication again and again – the SSO problem