Jan Camenisch, Sebastian Mödersheim, Gregory Neven, Franz-Stefan Preiss, Dieter Sommer

Credential-based access control extensions to XACML
Application identity management

Enterprise A

[Diagram of Enterprise A]
Enterprise identity management

Enterprise A

Enterprise B
Federated identity management

Enterprise A

Enterprise B

static mapping

© 2009 IBM Corporation  Gregory Neven, IBM Research – Zurich  W3C Workshop on Access Control Scenarios, Nov. 18th, 2009, Luxembourg
Collaborative identity management

Enterprise A

Enterprise B

IDP

IDP

IDP

Collaborative identity management
Trends in identity management

Degree of Interconnectivity

- Less Externally Connected
- More Externally Connected

Dynamic vs. Static Entity Lifecycle

- Dynamic
- Static

Enterprise Identity Management
Federated Identity Management
Collaborative Identity Management
Application Identity Management
### Trends in Identity Management

<table>
<thead>
<tr>
<th>Degree of Interconnectivity</th>
<th>Proprietary user DB</th>
<th>Internal LDAP</th>
<th>Application Identity Management</th>
<th>Kerberos tickets</th>
<th>RFID</th>
<th>X.509 certificates</th>
<th>SAML</th>
<th>Idemix, U-Prove</th>
<th>eID smartcards</th>
<th>Federation Identity Management</th>
<th>Collaborative Identity Management</th>
<th>Enterprise Identity Management</th>
<th>Enterprise Identity Management</th>
<th>Application Identity Management</th>
<th>Public LDAP</th>
<th>X.509 certificates</th>
<th>SAML</th>
<th>Idemix, U-Prove</th>
<th>eID smartcards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less Externally Connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Externally Connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trends in Identity Management

Credentials
Credentials

- Credential: list of attribute values, certified by issuer
- Attributes describe user's identity (e.g., identity card), user’s rights (e.g., credit card, concert ticket) or both (e.g., driver’s license)
- Example technologies:
  X.509, SAML, CardSpace, OpenID, Kerberos, LDAP, Idemix, U-Prove,…
- Possible additional features:
  - attribute authentication
  - proof of ownership
  - (selectively) reveal attributes
  - prove condition on attributes
  - (selectively) reveal attributes to third parties
  - sign statements
  - limited spending
Language requirements

- Reference to individual credentials, (attribute-id, issuer) doesn’t suffice
  - Credential types
    e.g. reveal name as on govt-issued passport, not ID card
    extensible OWL ontology of attributes and credential types
  - Credential mixing
    e.g. reveal number, expiration from same credit card
  - Cross-credential conditions
    e.g. passport.name = creditcard.name

- Distinguish between “reveal attribute” and “prove that condition holds”
  e.g. reveal birth date vs. age>18

- Provisional actions:
  Sign statements, reveal to 3rd party, limited spending
Example policy

own $p$::Passport issued-by USAgov
own $r$::ResidencePermit issued-by ChicagoTownhall
own $c$::CreditCard issued-by Visa,Amex
reveal $c$.number , $c$.expirationDate under ‘purpose=payment’
reveal $r$.address to ShippingCo under ‘purpose=shipping’
sign ‘I agree with the general terms and conditions.’
where $p$.dateOfBirth ≤ dateMinusYears(today(), 21) ^ $c$.expirationDate > today()
Embedding into XACML

[Diagram of XACML schema with labeled components and relationships]

Legend:
- Existing, unmodified XACML 3.0 element
- Existing XACML 3.0 element, modified schema
- New element, schema defined here
Embedding into SAML

- New SAML statement types to carry
  - conditions on attributes using `<xacml:Condition>`
  - provisional actions

- Extend SAML assertion authentication to any type of proof token, e.g.
  - `<ds:Signature>`
  - LDAP server/password
  - Idemix proof
  - …
Summary

- Credential-based access control
  - attributes grouped in credentials
  - show multiple credentials simultaneously
  - technology independence
- Privacy enhancements
  - reveal attributes vs. prove condition
  - support anonymous credentials
- Embedded into XACML & SAML