JSR 375 update
June 15, 2015

Werner Keil, Jean-Louis Monteiro
Why a Java EE Security JSR?

- Java EE 8 survey results
Survey Results

Should we standardize on requirements for simple security providers and their configuration?

- Yes: 65.2%
- No: 11.7%
- Not sure: 23.1%

Should we consider adding Security Interceptors in Java EE 8?

- Yes: 78.6%
- No: 7.1%
- Not sure: 14.3%

Should we standardize group-to-role mapping?

- Yes: 69.7%
- No: 7.7%
- Not sure: 22.6%

Should we simplify authorization by introducing an EL-enabled authorization annotation?

- Yes: 66.7%
- No: 10.5%
- Not sure: 22.8%
Survey Results – Password Aliasing

API for Password Aliasing

Should we add support for password aliases (including the ability to provision credentials along with the application)?

- Yes: 57.9%
- No: 11.5%
- Not sure: 30.6%

- Deferred from Java EE 7
## Planning – Epics

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminology</td>
<td>In Progress</td>
<td>Establish Security API terminology to enable accurate and concise communication</td>
</tr>
<tr>
<td>Authentication Mechanism</td>
<td>In Progress</td>
<td>Simplify application-accessible authentication mechanisms</td>
</tr>
<tr>
<td>Identity Store</td>
<td>In Progress</td>
<td>Standardize application-accessible identity store</td>
</tr>
<tr>
<td>Role/Permission Assignment</td>
<td>Not Started</td>
<td>Standardize application-accessible role/permission assignment</td>
</tr>
<tr>
<td>Security Context</td>
<td>Not Started</td>
<td>Standardize a platform-wide Security Context</td>
</tr>
<tr>
<td>Authorization Interceptors</td>
<td>Not Started</td>
<td>Standardize platform-wide Authorization Interceptors</td>
</tr>
<tr>
<td>Password Aliasing</td>
<td>Not Started</td>
<td>Standardize the API for using password aliases in configuration</td>
</tr>
<tr>
<td>Standardized Server</td>
<td>Not Started</td>
<td>Using the simplified Authentication Mechanism, standardize some additional ServerAuthModules</td>
</tr>
</tbody>
</table>

See: [https://java.net/projects/javaee-security-spec/pages/Home](https://java.net/projects/javaee-security-spec/pages/Home)
Ideas

To modernize, standardize, simplify

- Identity Store
- Authentication Mechanism
- Security Context
- Role/Permission Assignment
- Authorization Interceptors
- Password Aliasing
OpenID Connect ServerAuthModule

@Authenticator("javax.security.authenticator.OpenIDConnect")
@WebServlet("/SimpleServlet")
@ServletSecurity(@HttpConstraint(rolesAllowed = {"manager"}))
public class SimpleServlet extends HttpServlet {
    @Override
    protected void doGet(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
        response.getWriter().print("my GET");
    }
}
Ideas – Authentication Events

- Throw standardized CDI events at important moments
  - PreAuthenticate Event
  - PostAuthenticate Event
  - PreLogout Event
  - PostLogout Event
Ideas – Authentication Event Usage

● Possible Use Cases
  ○ Tracking number of logged-in users
  ○ Tracking failed login attempts per account
  ○ Side effects, like creating a new local user after initial successful authentication via a remote authentication provider
  ○ Loading application-specific user preferences
  ...
Ideas – Identity Management

- Application manages its own users and groups
- Need to access a repository of identities, like users
- Users may be stored in app-specified repository (e.g. LDAP)
- Users are managed without access to server configuration
Ideas – Identity Management

Identity

IdentityStore

LDAP
File
DB
Server
Identity Management

Current Solutions

- No Java EE support
- Only proprietary server support
- 3rd party security frameworks provide user/group APIs
IDM – Components
Identity Management components should be injectable via CDI.

<table>
<thead>
<tr>
<th>Component</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Manager</td>
<td>@ApplicationScoped</td>
</tr>
<tr>
<td>Identity Manager</td>
<td>@RequestScoped</td>
</tr>
<tr>
<td>Relationship Manager</td>
<td>@RequestScoped</td>
</tr>
</tbody>
</table>
IDM – Java EE Identity Model
IDM – Credential Validation
Links

- Java.net Project Page: https://java.net/projects/javaee-security-spec
- Users Mailing List: users@javaee-security-spec.java.net
- Github Playground: https://github.com/javaee-security-spec/javaee-security-proposals