# Role-based Access Control in Federated Environments

**Satish Vellanki**

## Problem Description

- No mechanism to create authorized service federations in SORCER
- No uniform access control across explicit administration boundaries
- No user-centric access control while global permissions defined around administration domains
- PKI creates global namespace with CA
- PKI does not provide delegated authorization

*A flexible role-based access control crossing administration boundaries and around users is needed in metacomputing environment.*

## Objective/Approach

**Objective**

Role-based access control framework (RACF) in SORCER

**Approach**

- Review and analyze existing role-based solutions
- Define requirements for RACF in SORCER
- Develop role-based access control protocol
- Design RACF
- Implement RACF
- Verify & validate RACF
- Deploy RACF in the SORCER environment

## Schedule

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature Review</td>
<td>03/2007</td>
</tr>
<tr>
<td>RACF Requirements Definition</td>
<td>04/2007</td>
</tr>
<tr>
<td>RACF Access Control Protocol</td>
<td>06/2007</td>
</tr>
<tr>
<td>Design and Implementation</td>
<td>09/2007</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>10/2007</td>
</tr>
<tr>
<td>Deployment in SORCER</td>
<td>11/2007</td>
</tr>
</tbody>
</table>

## Benefits

- Secure access to protected resources in federated environment
- Flexibility in granting rights by users to other users
- Zero administration in the user-centric framework
- Intuitive and user friendly interface supporting role-based access