**Problem Statement**

- File-based storage of large amount of keys does not provide efficient access control in a metacomputing environment.
- Having large number of key files and large number of passwords to access keystore files and keys becomes unmanageable in large S2S environments.
- Inefficient local management of large number of public keys by each service provider collaborating with large number of other service providers.
- When keystore files become not available the security cannot be reinforced.

**Objective**

A Scalable Key Management Framework (SKEMAF) for centrally managed and replicated keys in metacomputing environments.

**Approach**

- Review Literature
  - Key storage and usage
  - Keystore in Client/Service and Peer-to-Peer environments
- Define requirements for SKEMAF
- Analyze data structures and storages representation for central SKEMAF
- Develop SKEMAF methodology
- Design SKEMAF and corresponding model
- Implement and deploy SKEMAF
- Verify and Validate SKEMAF

**Schedule**

<table>
<thead>
<tr>
<th>Literature Review Report</th>
<th>October 10, 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements for SKEMAF - UML Diagram</td>
<td>October 31, 2007</td>
</tr>
<tr>
<td>SKEMAF Methodology - Use Cases and Architecture</td>
<td>November 15, 2007</td>
</tr>
<tr>
<td>SKEMAF UML Component Diagram</td>
<td>November 30, 2007</td>
</tr>
<tr>
<td>Proposal Presentation</td>
<td>December 2007</td>
</tr>
<tr>
<td>SKEMAF Implementation</td>
<td>February 2007</td>
</tr>
<tr>
<td>User Agent for Managing Providers Keys</td>
<td>March 2007</td>
</tr>
<tr>
<td>Verification and Validation of SKEMAF</td>
<td>April 2007</td>
</tr>
</tbody>
</table>

**Benefits**

- Uniform and centralized creation and verification of digital signatures.
- Scalable and reliable federated key management system by replicated central storage.
- Simplified, flexible and efficient management of keys by central keystore services.
- Friendly and intuitive user interface to create and manage keys.
- Keystore maybe used as certificate authority.