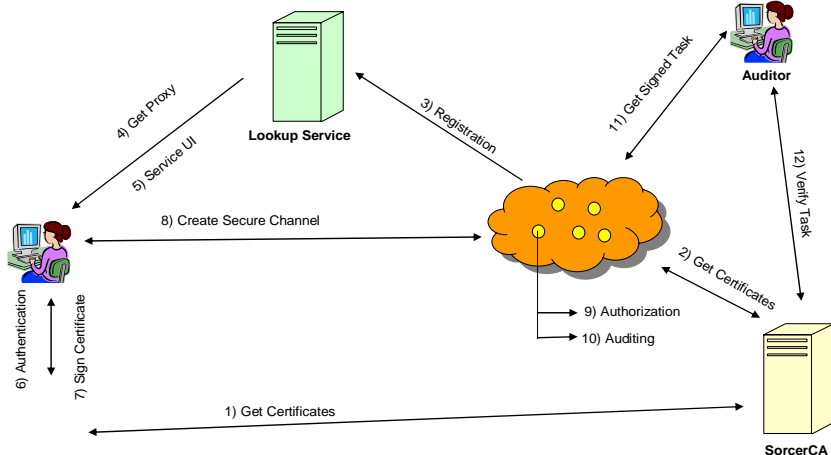# Smart Card Authentication and Authorization Framework (SCAF)
Saurabh Bhatla

Problem Description

- User credentials are not intrusion protected and are not portable
- Service-oriented computing environments are not secure
    - Mutual authentication does not scale with large number of requestors
    - Authorization is does not scale with large number of services

Smart cards are needed to provide reliable credentials for mutual authentication and authorization in Service-Oriented Environment

Objective/Approach

Objectives:

- Select CA to support PKI infrastructure
- Define use cases for SCAF
- Define user credentials for SO Computing
- Architect SO environment for SCAF
- Design the framework for authentication, authorization, and non-repudiation
- Design a service requestor and provider to validate SCAF

Approach:

- Deploy CA to issue provider/requestor credentials
- Populate requestor credentials on smart card
- Develop and deploy SCAF in the SORCER environment
- Develop a service-oriented application: Bulletin Board
- Validate the framework with the Bulletin Board application

Schedule

Background research	10/07/2004
Smart card implementation	10/15/2004
Authentication and identification	10/25/2004
SSL endpoint implementation	11/15/2004
Requestor authorization	11/30/2004
Proposal presentation	12/20/2004
Verification/CA deployment	12/25/2004
Thesis defense and demo	03/01/2005

Benefits

- Safeguarding user integrity, passwords are safely stored on smart cards
- Preventing credential intrusion
- Scalability for unlimited number of providers/requestors
- Cost effective with own CA
- Reliable authentication in SO frameworks
- Flexible multilayered authorization using JAAS
- Secure communication between ServiceUI and Service Provider
- Trusted zero install requestor ServiceUI with JavaCardLoginModule