

# SOA REFERENCE ARCHITECTURE: ENTERPRISE SECURITY

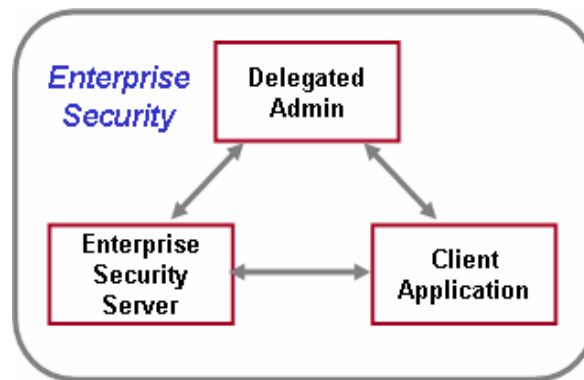
## SOA Blueprint

A structured blog by Yogish Pai

### Enterprise Security

Currently most packaged or custom applications implement their own security solutions. However, when an enterprise has multiple applications, each with its own authentication implementation, problems can arise when different authentication implementations are updated at different times.

This could be simplified by dividing enterprise security into three major components:



**Enterprise Security Components**

**Delegated administration:** user and resource administration application that enables administrators to create, modify, and delete user privileges as appropriate to their role. This application updates the same repository leveraged by the enterprise security server.

**Client applications:** externalize and leverage the enterprise security services.

**Enterprise security server:** provides security services such as user authentication, user identity management, authorization, auditing, user profile management, and user provisioning.

- Authentication validates the identity of a user through several authentication mechanisms. Identity can be validated against a password, or through digital certificates or smart cards. In the interests of productivity, users should need to be able to sign on once and gain access to multiple resources, but enterprises need to implement proper controls and policies so that, once authenticated, users can access only the resources they're authorized to work with.
- Identity management maps multiple identities to a single user or links identities across applications to support coexistence of multiple user identities.
- Authorization involves controlling access of users to diverse resources across the enterprise.
- Auditing involves tracking user activities.
- Profile management involves managing the profiles of the users.
- Provisioning automates the time-consuming process of managing accounts and their life cycles. It allows centralized activation, modification, or deactivation of accounts across multiple applications in an enterprise. User provisioning could include explicit granting or revoking of user access to resources and establishing of entitlement policies for the user.



## **Copyright**

Copyright © 2007.

The author grants a non-exclusive licence to everyone to publish this document in full or part by acknowledging the source. Any other usage is prohibited without the express permission of the authors.

