# Business layer

# Cross – cutting concerns

- Authentication
- Authorization
- Caching
- Communication, exception management
- Logging and instrumentation
- Validation

# …where mistakes are most often made

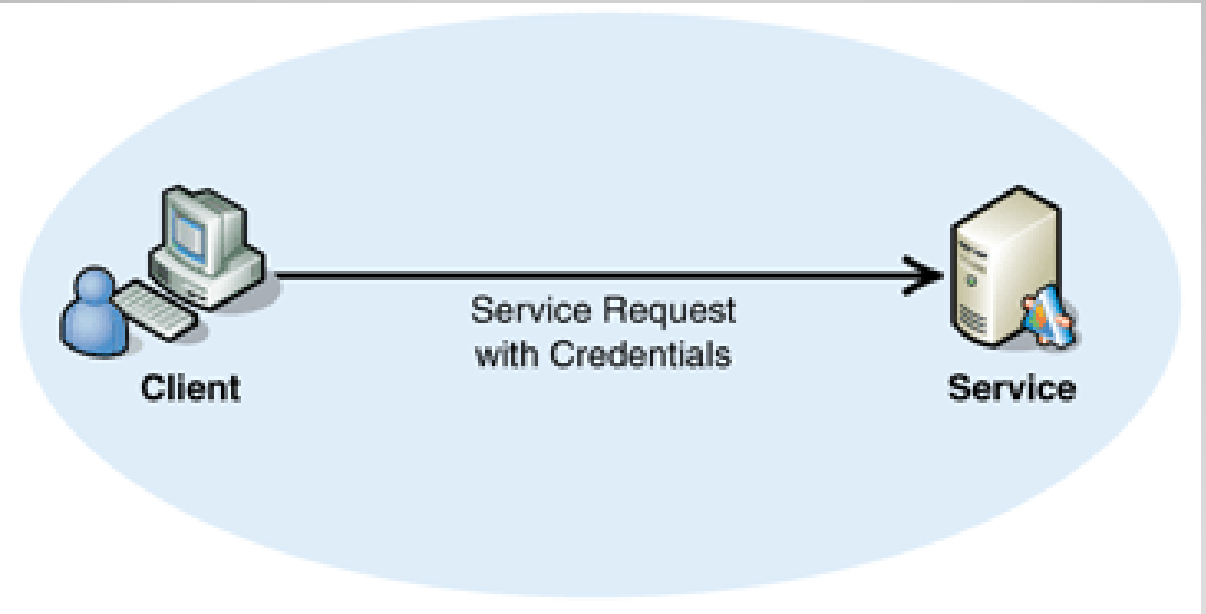
Authentication and Authorization

- Lack of authentication across trust boundaries
- Lack of authorization across trust boundaries
- Granular or improper authorization

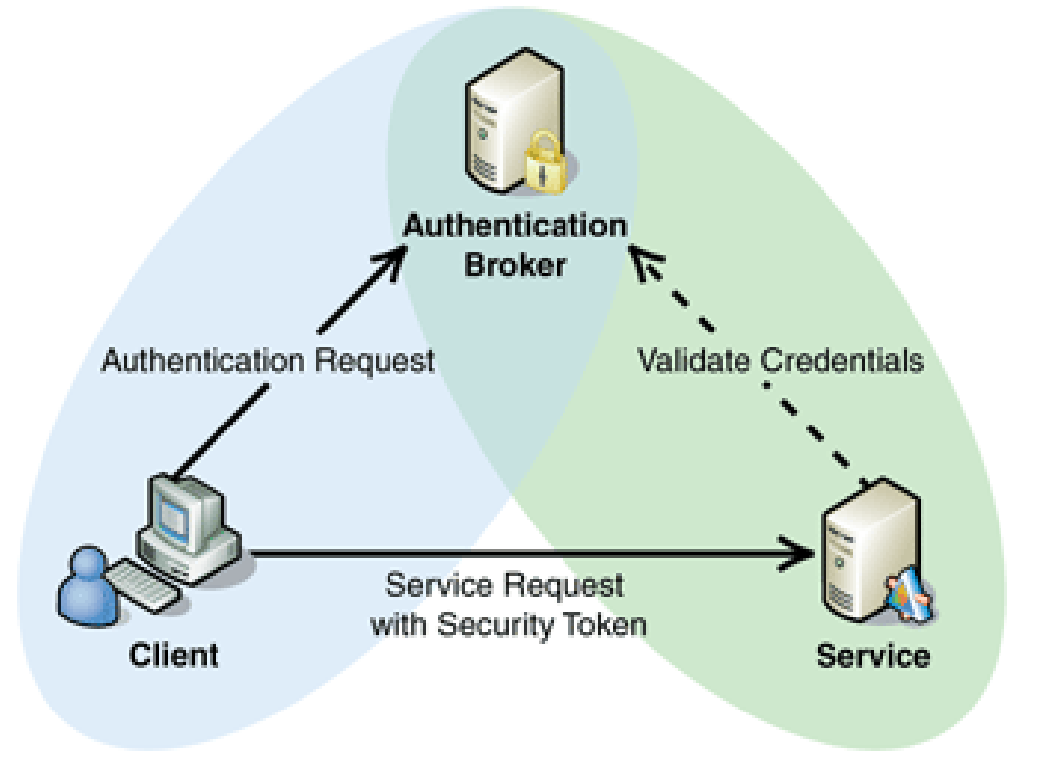
# Authentication guidelines

- Identify your trust boundaries
- Enforce the use of strong passwords or password phrases
- Consider a single sign-on strategy
- Do not transmit passwords over the wire in plain text

# Direct vs. Brokered Authentication



# Direct vs. Brokered Authentication



# Authorization guidelines

**Consider the following guidelines when designing an authorization strategy:**

- Identify your trust boundaries and authorize users and callers across the trust boundary
- Protect resources by applying authorization to callers based on their identity, groups, or roles
- Use role-based authorization for business decisions
- Use resource-based authorization for system auditing
- Use claims-based authorization when you need to support federated authorization based on a mixture of information such as identity, role, permissions, rights, and other factors