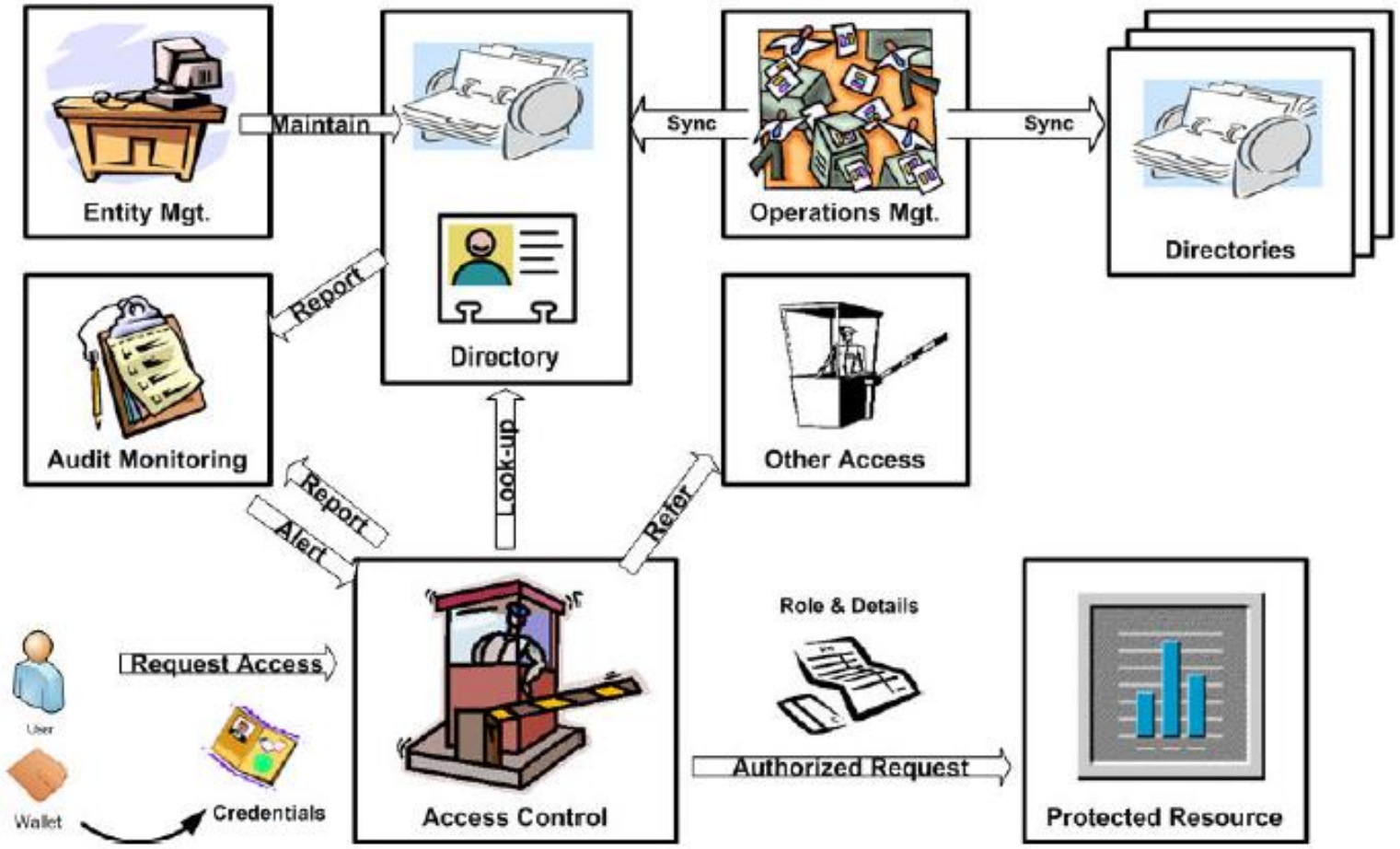
CISSP Study Group:
Identity and Access Management (IAM)

Scott Forbes (CISSP, CSSLP)

CISSP Domain #5
Identity and Access Management

A. Physical and logical assets control
B. Identification and authentication of people and devices
C. Identity as a service (e.g. cloud identity)
D. Third-party identity services (e.g. on-premise)
E. Authorization mechanisms
F. Access control attacks
G. Identity and access provisioning lifecycle (e.g. provisioning review)

Identity and Access Management Conceptual Model



AAA

- Authentication (AuthN)
  - Who is doing the activity
- Authorization (AuthZ)
  - What can they do
- Accounting (Audit)
  - Who/What/When/Where did it happen

5A: Physical and Logical Access

- Subject (Ex: User)
- Object (Ex: File)
- Access Controls
  - Preventative (Try to prohibit)
  - Deterrent (Try do discourage)
  - Detective
  - Corrective
  - Etc…

5B: Identification & Authentication

Identification

- "Claiming" an Identity
  - I am "Scott Forbes"
  - I am user "scottf"

Authentication (AuthN)

- "Verifying" the claim
  - Something you Know
  - Something you Have
  - Something you Are
    - Biometric Accuracy
      - False Reject Rate (FRR)
      - False Acceptance Rate (FAR)
      - Crossover Error Rate (CER)
  - Multi-Factor

Directories

- "Special" kinds of databases
  - Optimized for Search/Read access
  - Replicated and synchronized
  - Highly Available
  - Shared
  - "Owned" by Ops, not AppDev
- Enterprise Roles/Groups
  - Typically not fine-grained Application Roles
- Examples
  - Microsoft Active Directory
  - X.500 Directory Service
  - Lightweight Directory Access Protocol (LDAP)

Authorization (AuthZ)

- Functional (What can I do)
  - Create, Read, Update, Delete (CRUD)
- Data (What objects can I access)
  - Accounts
  - Users (Manager sees their direct reports)

Distributed Applications and Organizations

- Centralized Access Control
- Distributed Access Control
- Single Sign On (SSO) within an Organization
- Federated Access Control
  - SAML
  - Other token based authentication
  - Kerboros
  - SESAME
  - RADIUS
  - Diameter
  - TACACS(+)
  - PAP and CHAP

Digital Certificates

- Server Authentication
  - HTTPS: Server Certificate
- Client Authentication
  - HTTPS: w/ Client Certificate
- Secure Shell (SSH) Keys
  - Generate a public-private key pair on the server
  - Install the public key on your SSH client(s)
  - Configure SSH software to authN with the server key

Federated IdM

http://www.softwaresecured.com/2013/07/16/federated-identities-openid-vs-saml-vs-oauth/

- SAML:
  - Service Provider (SP) asks ID provider (IdP) to authenticate the Principle (P) with signed request containing the Security Assertion(I am scott@abc.com)
- OpenID: Federated Identification/AuthN
- OAuth2: Federated AuthZ

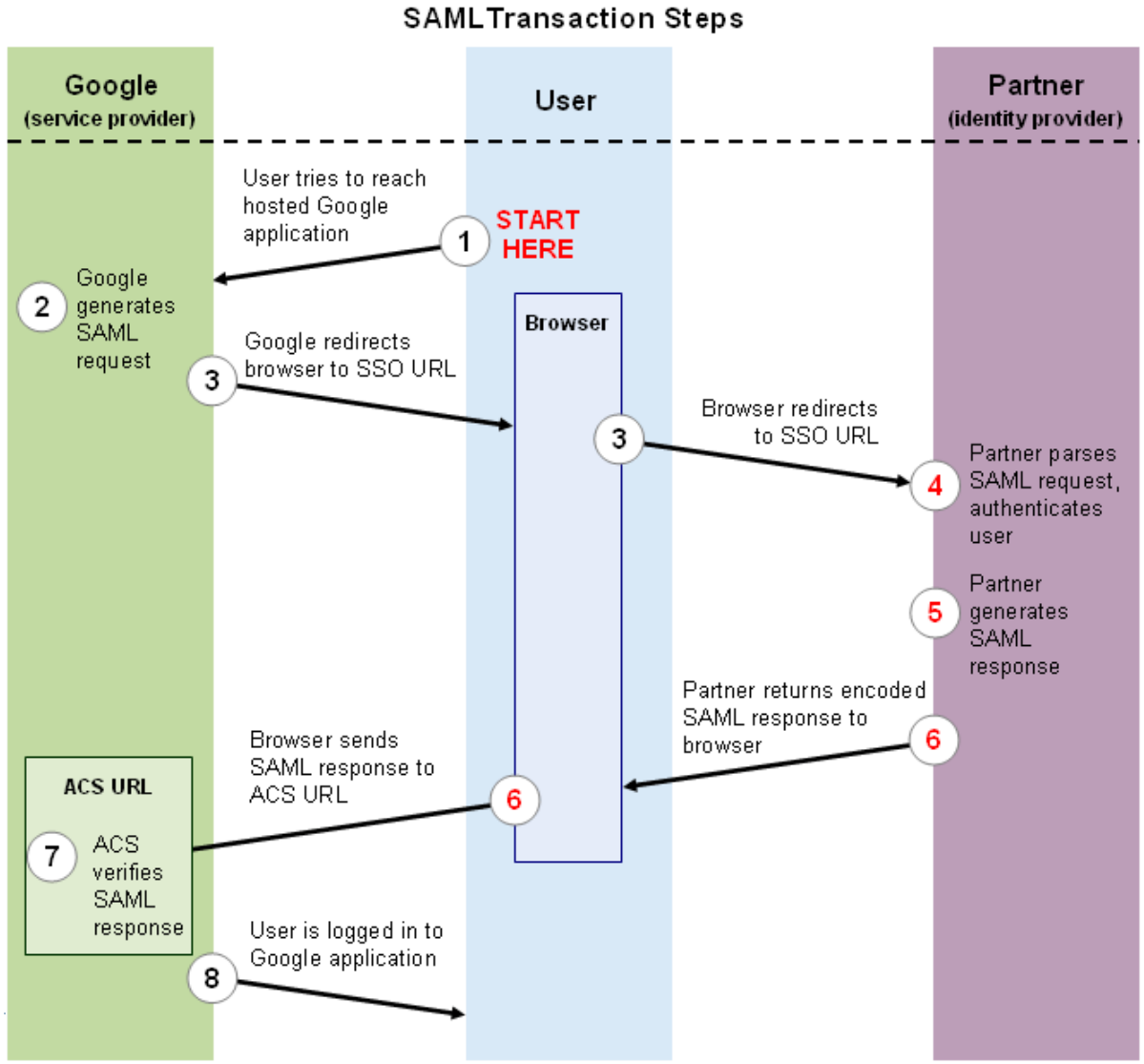
5C: Identity as a service (IDaaS)

Figure 1. Magic Quadrant for Identity and Access Management as a Service

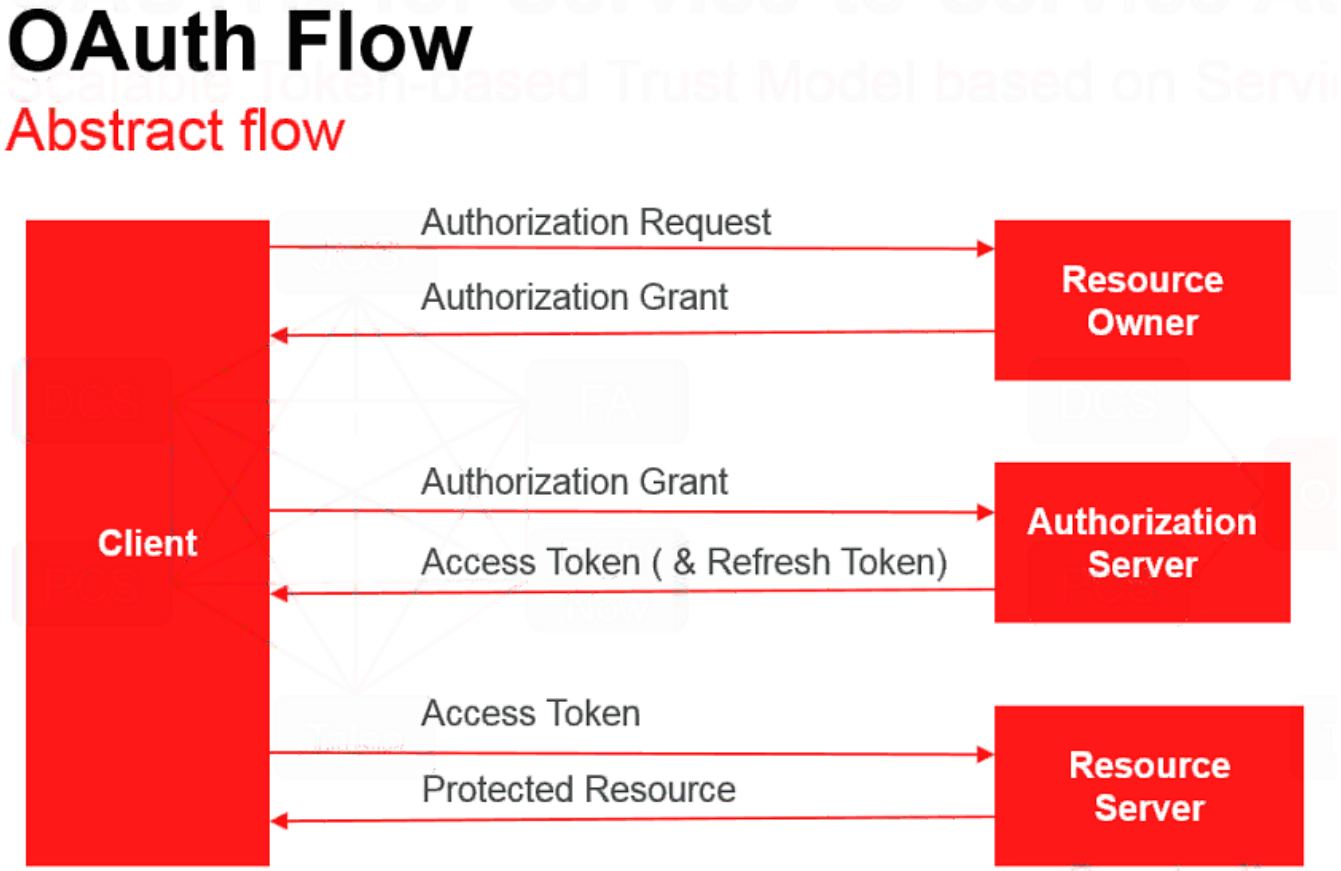
5D: Third-party identity services

- Cloud Identity
- Directory Sync
- Federated Identity

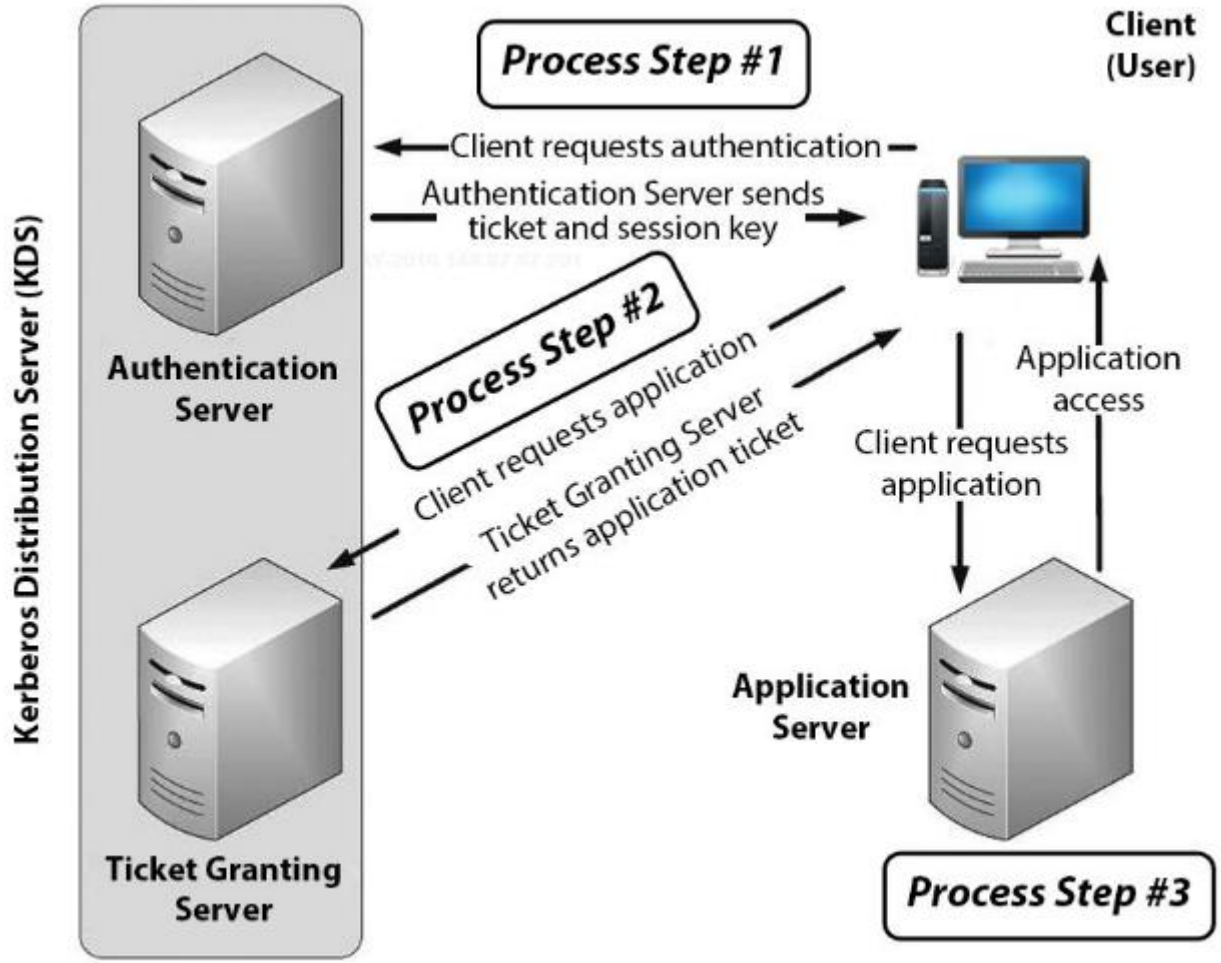
SAML:
Security Assertion Markup Language



OAuth2


OAuth Flow
Abstract flow
Client
Authorization Request
Authorization Grant
Resource Owner
Authorization Grant
Access Token (& Refresh Token)
Authorization Server
Access Token
Protected Resource
Resource Server

Kerberos

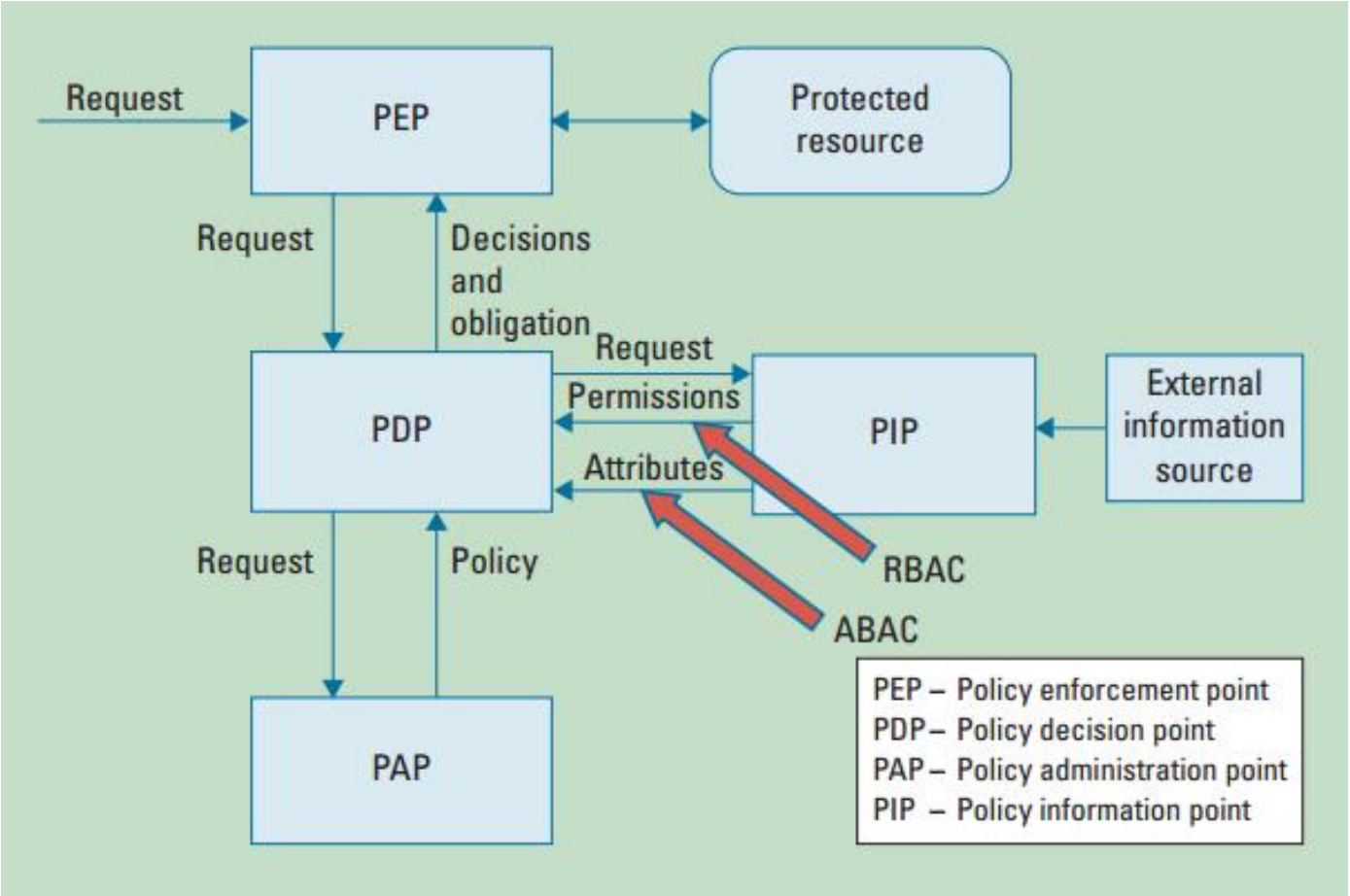

Kerberos Distribution Server (KDS)
Authentication Server
Ticket Granting Server
Process Step #1
Client requests authentication
Authentication Server sends ticket and session key
Client (User)
Process Step #2
Client requests application
Ticket Granting Server returns application ticket
Application access
Client requests application
Application Server
Process Step #3

5E: AuthZ Mechanisms

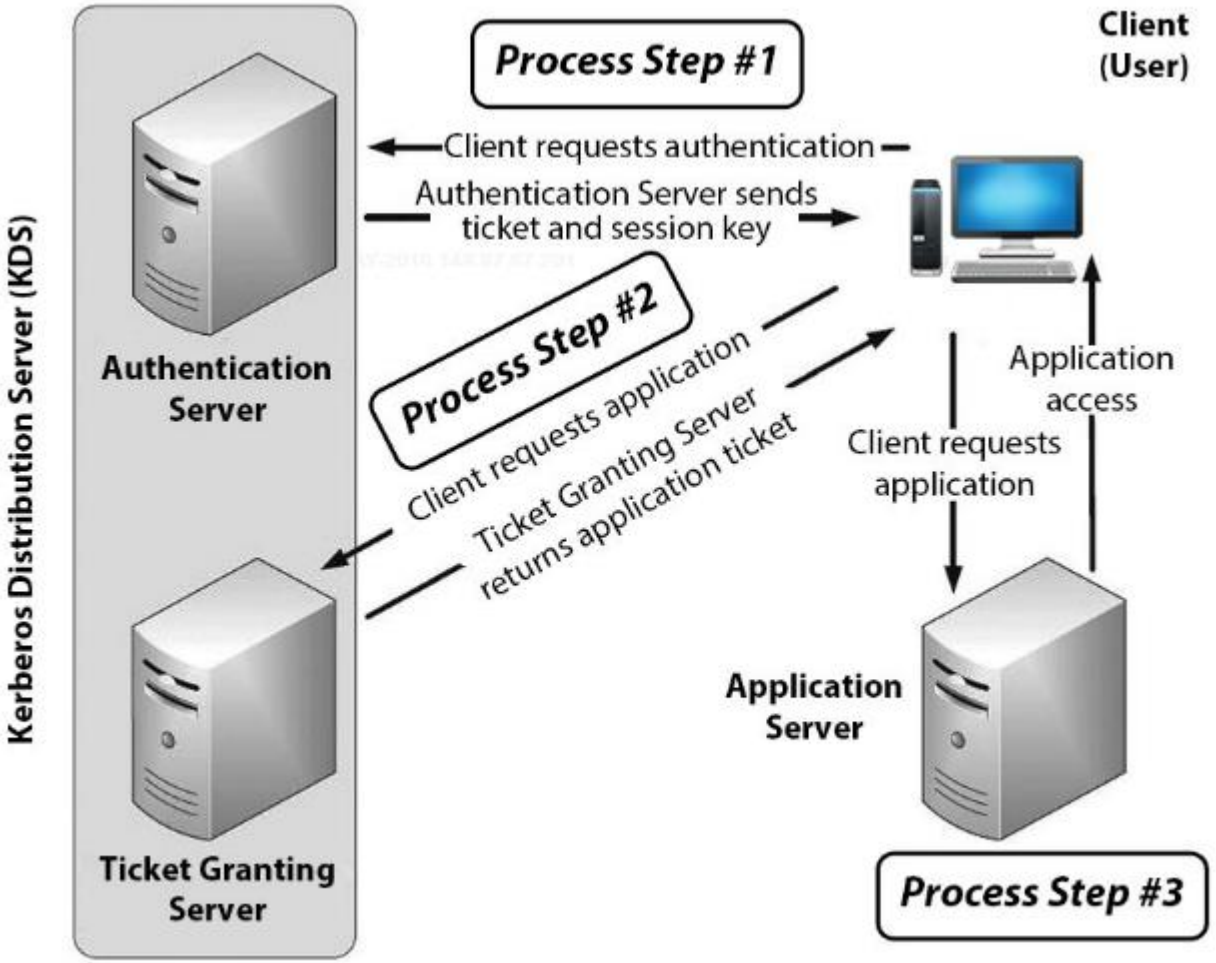
- Discretionary Access Control (DAC)
  - Data Owner grants access to others as they choose
- Mandatory Access Control (MAC)
  - Central Security grants access to specific users
- Role-Based Access Control (RBAC)
  - Group is a collection of users and/or other groups
    - Makes it easier to manage similar users
  - Role is a collection of permissions and/or other roles
    - Roles can be modified by time of day, location of access, etc.
- Attribute Based Access Control (ABAC)
  - Access is controled by attributes of the resource.

Enforcing RBAC and ABAC

See: ABAC and RBAC - NIST



Kerberos: Network AuthN Protocol
See: CISSP CBK



5F: Access control attacks

- Control Physical Access
- Protect Credentials
  - One-Way Encryption (aka Hashing) is best practice
- Muti-factor AuthN
- Account Lockout or Throttling
- Last Login Notification
- Educate Users
- Audit Access
- Manage Accounts
- Vulnerability Scanners

5G: Access Provisioning Lifecycle

- Provisioning
- Review
- Revocation