DCE: Sicherheit

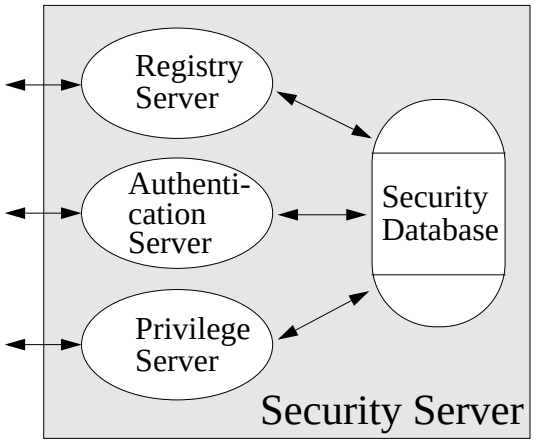
- Verwendung des Kerberos-Protokolls
  - Vertraulichkeit durch Sitzungsschlüssel (--> DES)
  - gegenseitige Authentifizierung
  - selektive Autorisierung von Clients für bestimmte Dienste
  - Schlüsselverwaltung
  - zusätzlich auch asymmetrische Verfahren (“public key”)

- Wählbare Sicherheitsstufen bei der Kommunikation
  - Authentifizierung nur bei Aufbau der Verbindung (“binding”)
  - Authentifizierung pro RPC-Aufruf
  - Authentifizierung pro Nachrichtenpaket
  - Zusätzlich Verschlüsselung jedes Nachrichtenpaketes
  - Schutz gegen Verfälschung (verschlüsselte Prüfsumme)

- Autorisierung ist mittels Zugriffkontroll-Listen realisiert
  - es gibt zahlreiche verschiedene Typen von Rechten
  - Gruppenbildung von Benutzern / Clients möglich
  - ACL-Manager bei den Servern verwaltet lokale Kontroll-Listen
  - Clients schicken eine verschlüsselte, authentische und gegen Replays gesicherte Repräsentation ihrer Rechte mit jedem Aufruf mit (PAC = Privilege Attribute Certificate); wird vom ACL-Manager überprüft

- Werkzeuge zur Systemadministration
  - Eintragen / Ändern von Rechten etc.
  - Installation zellübergreifender Sicherheitsdienste
  - hierzu spezieller “Registry-Server”

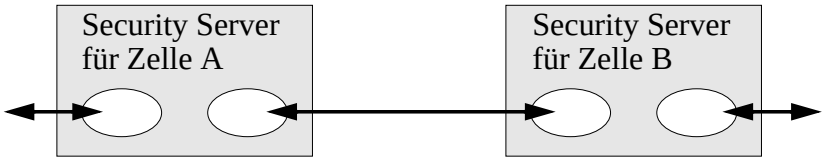
DCE-Sicherheitsdienste



- *Registry Server:* Verwaltung von Benutzerrechten; Dienste für Systemverwaltung
- *Datenbasis* enthält private Schlüssel (u.a. Passwörter in verschlüsselter Form...)
- *Privilege-Server* überprüft Zugangsberechtigung; u.a. bei login

- Sicherheitsdienst kann *repliziert* werden, um hohe Verfügbarkeit zu erreichen
  - nur Primärkopie kann Daten aktualisieren, Replikate sind “read only”
  - Primärkopie aktualisiert gezielt die Replikate

- *Zellenübergreifende Sicherheitsdienste:*



- ein Security Server A nimmt gegenüber einem Security Server B eine Clientrolle ein (“vertritt” die Clients seiner Zelle)
- ein Security Server besitzt im Gegensatz zu anderen Clients nicht einen einzigen geheimen Schlüssel, sondern es werden paarweise spezifische Schlüssel (“Surrogate”) vereinbart

Weitere DCE-Komponenten

- Cell Directory Service (CDS)
  - realisiert Zuordnung von Namen und Adressen
  - verwaltet Namen (mit Attributen) einer Zelle
  - Beispiel für Attribute: *Druckername*, *Standort*, *Art* für einen Drucker (mit spezifischen Werten z.B. *pr99*, *Raum7*, *color600dpi*)
  - Replikation (zwecks Fehlertoleranz) möglich (dabei “Konvergenzlevel” einstellbar)

- Global Directory Service (GDS)
  - Bindeglied zwischen verschiedenen CDS
  - hierarchischer Namensraum
  - Namenformat basiert auf X.500 oder DNS

Namensverwaltung

- Distributed File System (DFS)
  - ortstransparenter Dateizugriff
  - Caching beim Client steigert Effizienz (“Session-Semantik”)
  - mehrere Read-only-Replikate möglich
  - Unterstützung von Recovery, Migration und Backup
  - Synchronisation gleichzeitiger Zugriffsversuche
  - Gruppierung durch “File Sets“ (Gruppen von Dateien, die zusammen gelagert werden sollten)
  - nutzt DCE-RPC

- Distributed Time Service (DTS)
  - Synchronisationsprotokoll zwischen mehreren lokalen Zeitservern
  - Einbeziehung externer Zeitgeber (z.B. Funk- und Atomuhren)
  - Kopplung mit NTP-Protokoll möglich

DCE: Pragmatisches

Es gibt verschiedene Administrationstools
- Anzeigen und verändern von Information
- command line interface oder graphische Benutzungsoberfläche

---

Kritik an DCE: Komplexität
- Funktionsfülle (> 200 Funktionen)
  - wann benutzt man was?
  - Problem der wechselseitigen Beeinflussung („feature Interaction“)
  - Semantik bei Kombination verschiedener Mechanismen u.U. unklar
- Grösse
- mangelnde Effizienz