Wichtigste Fragen: Was ist notwendig, was wird gebraucht, was wäre auch noch gut?

Interne PKI oder externe

- Welche Produkte
    - Können Microsofts Certificate Services alle Anforderungen erfüllen?
- Absicherung der Private Keys
- Berechtigungskonzept
- Mehrstufigkeit

Wofür werden Zertifikate benötigt?

- Benutzer / Clients / Server
    - Zertifikatsparameter: Naming, Algorithm, Key Length, Life Time

Wie werden Zertifikate verwaltet?

- Verteilmechanismen
  Das Standard Protokoll ist wohl für die meisten Zertifikate im MS Umfeld RPC. Entweder für das Auto-Enrollment oder manuell via Microsoft Management Console (mmc).
    - RPC
    - SCEP
    - http (WebInterface / WebService)
    - Manuell / Skripte

  Eine Alternative für RPC ist es, den Web-Service und damit den CA Server nur via https für Clients erreichbar zu machen. Das schliesst Angriffslücken und reduziert Angriffsfläche.

- Die Ausstelllung von Zertifikaten
    - CA Approval
    - Enrollment Agent (signature certificate)
    - Permission

- Zurückziehen, Ablaufdatum kontrollieren, Renewing