http://www.densemode.com

Microsoft Two level PKI Hierarchy Workflow

Plan implementation

- naming conventions
  - common name for your CAs etc
- configuration
- encryption key type and size
  - hashing algorithm
    - use at least sha256
  - Change defaults for
    - certificate validity
      - 20 for root, 10 for issuing CA
    - crl validity on root
      - 20 years then no need to update crl unless revoking an issuing ca
- create text blocks for
  - capolicy.inf
  - AIA and CDP fields
  - certutil commands

Set up infrastructure

- set up base windows installations
- Name and join enterprise CAs, and CDP/OCSP server to AD
- Set up IIS server
  - pki folder
  - share and fs permissions
  - install IIS
  - create virtual directory
    - allow browsing
    - allow double escape

http://www.densemode.com

Two level PKI Hierarchy Workflow Contd.

Set up offline root CA

- Create capolicy.inf (optional)
- install services
- configure extensions
- run scripts
- publish crl
- copy root cert and crl to web server and issuing CA

Set up enterprise issuing CA

- Create capolicy.inf (optional)
- publish root Cert to AD
- add root cert and CRL to local store
- install services
- configure extensions
- run scripts
- copy enterprise cert to web server and rename
- publish CRL and Delta CRL

Configure Online responder for CA

- Install online responder
- Configure online responder for issuing CA

Create and test templates

- Create templates
    - issue templates
    - enroll devices
    - inspect certificates

Verify PKI

- use pkiview.msc to check for errors
- inspect certificates:
    - offline root
    - enterprise root

- certificates issued from templates

(Optional) configure AutoEnrollment GPO

- Scope policy to OU
- Scope templates using Access control Entries on Template