

# Are Off-line Root CAs Safer than On-line CAs?

David A. Cooper  
NIST

April 5, 2006

# What is an Off-line CA?

---

- Disconnected from network
- Turned off most of the time
- **Issues CRLs infrequently (e.g., once a month).**
- Only issues CA certificates
- **Public key of CA is used as trust anchor**

# Benefits of Off-line CA

---

- Risk of key compromise is reduced:
  - Completely protected from network attacks
  - Can provide greater protection from local attacks since access to the CA is needed infrequently.
  - Other benefits?

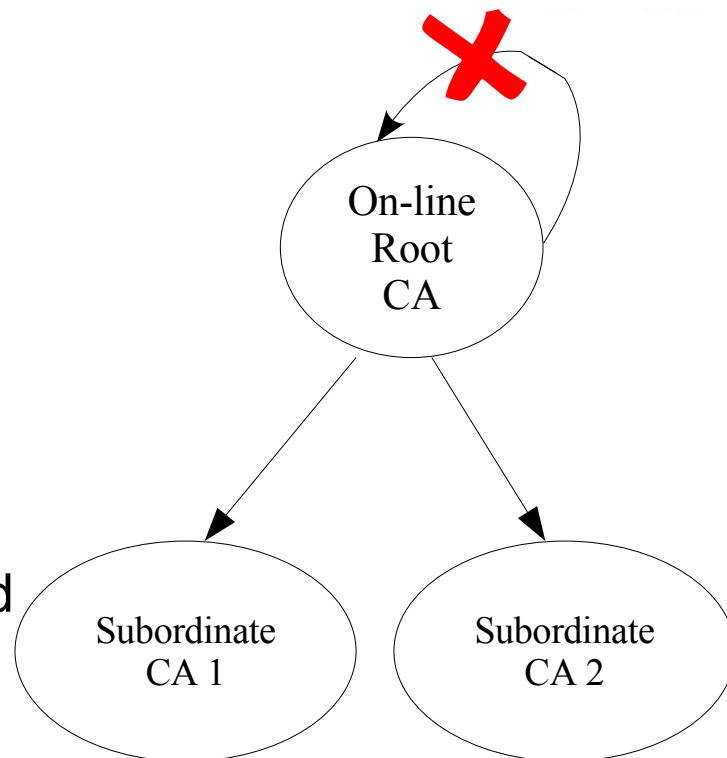
# Option 1: On-line CA

## ● Risk:

- Increased risk of compromise of root CA's key
- If root CA's key is compromised, all relying parties who use CA as trust anchor must be notified out-of-band

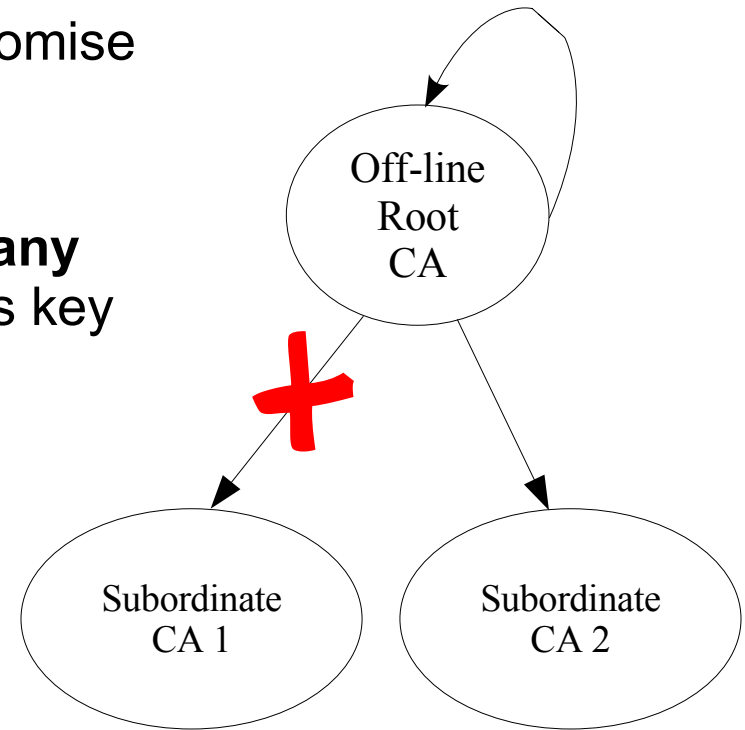
## ● Benefit:

- Out-of-band notification not required if a subordinate CA's key is compromised



# Option 2: Off-line CA

- Benefit:
  - Reduced risk of root CA key compromise
- Risk:
  - Out-of-band notification required if **any** subordinate (or cross-certified) CA's key is compromised



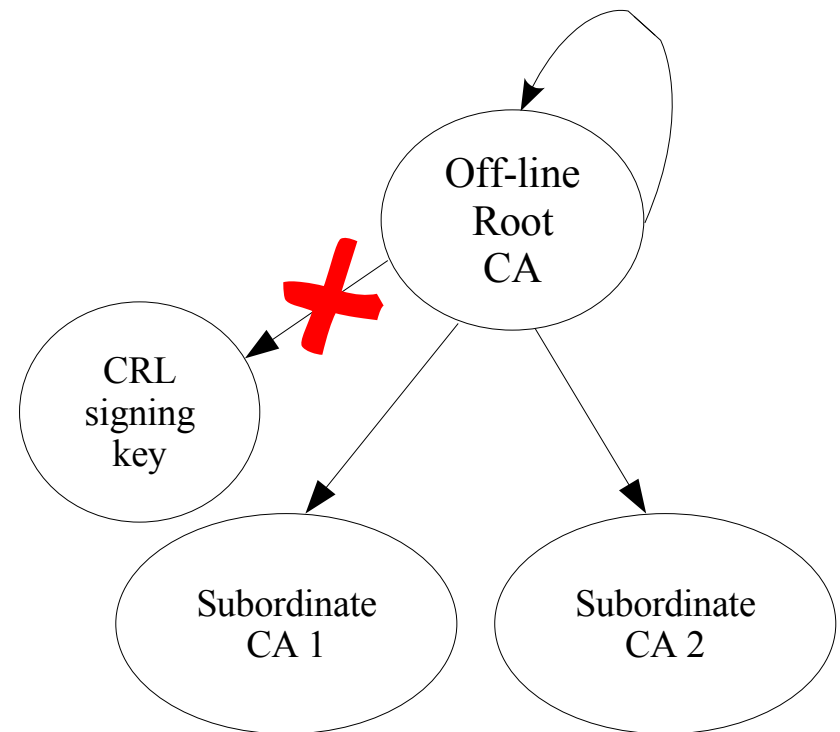
# Option 3: Off-line CA with On-line CRL Issuer

## Benefit:

- Reduced risk of root CA key compromise
- Out-of-band notification not required if a subordinate CA's key is compromised

## Risk:

- Out-of-band notification required if CRL signing key is compromised
- Path validation more complicated



# Does the use of an off-line root CA really improve security?

