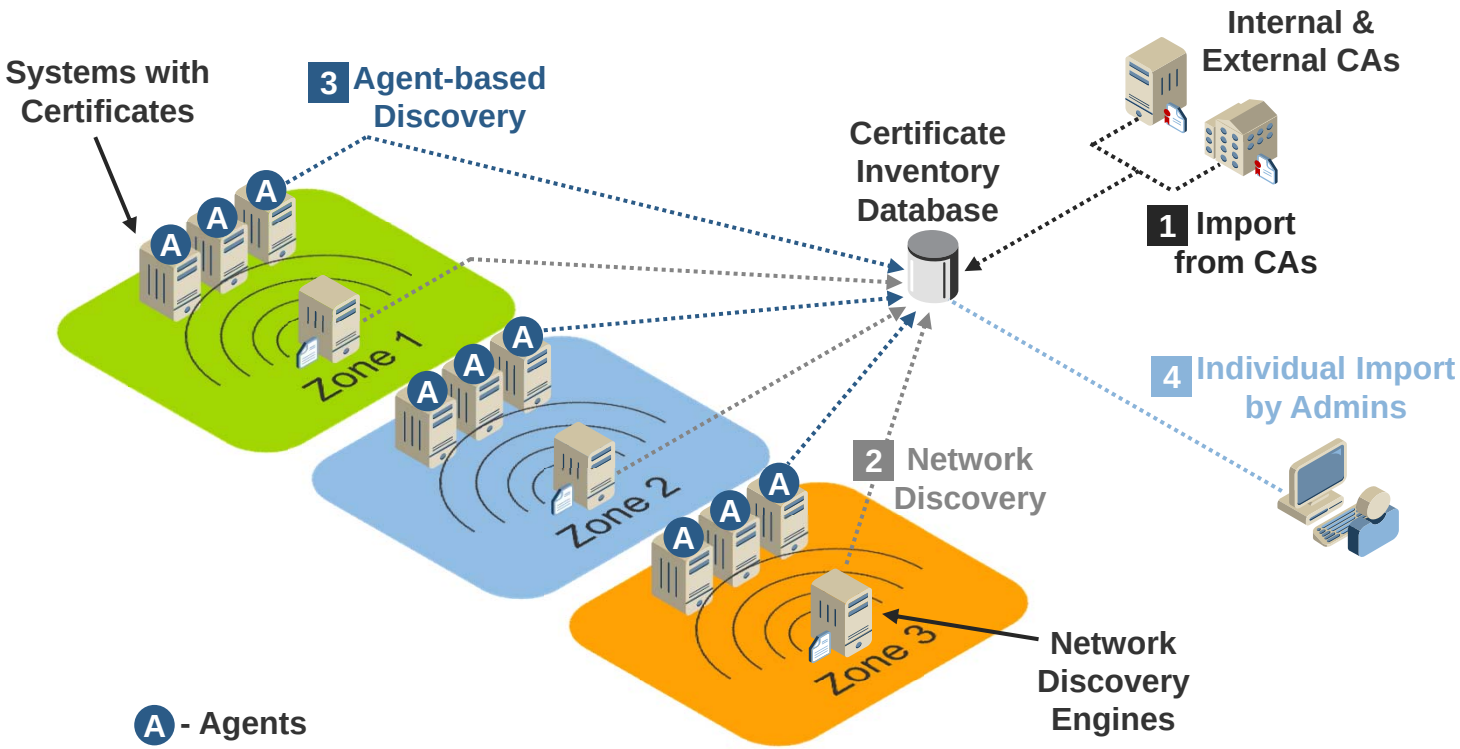
Establishing a Comprehensive Inventory

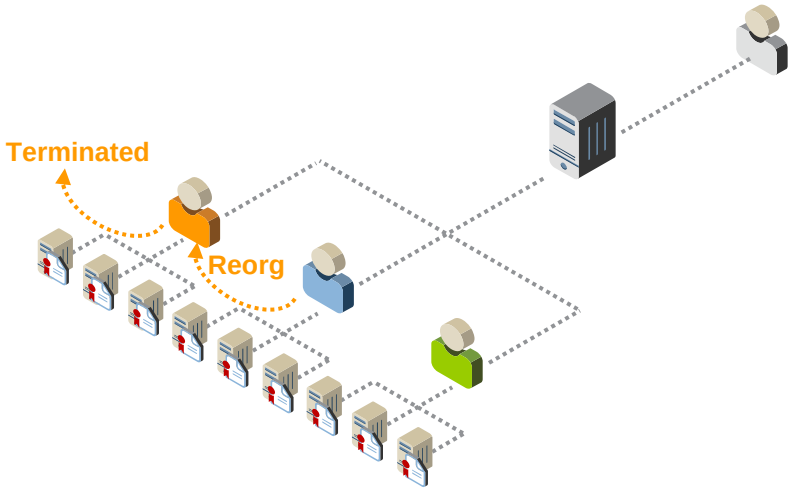


Analyze Inventory and Evaluate Compliance

- Certificate authorities/self-signed certificates
- Key lengths
- Signing hash algorithms (e.g. MD5 or SHA1)
- Validity periods
- Expiration dates
- Locations
- Keystore types
- Owners
- Business applications
- Applicable policies and regulations
- Current management processes

Managing Ownership Information

- It is critical to have up-to-date ownership information
  - Notifications for expirations
  - Notifications in case of compromise
  - Invalid notification is worse than no notification at all
- Best to have owners directly manage the updating of information
- Provide central oversight and support



Summary

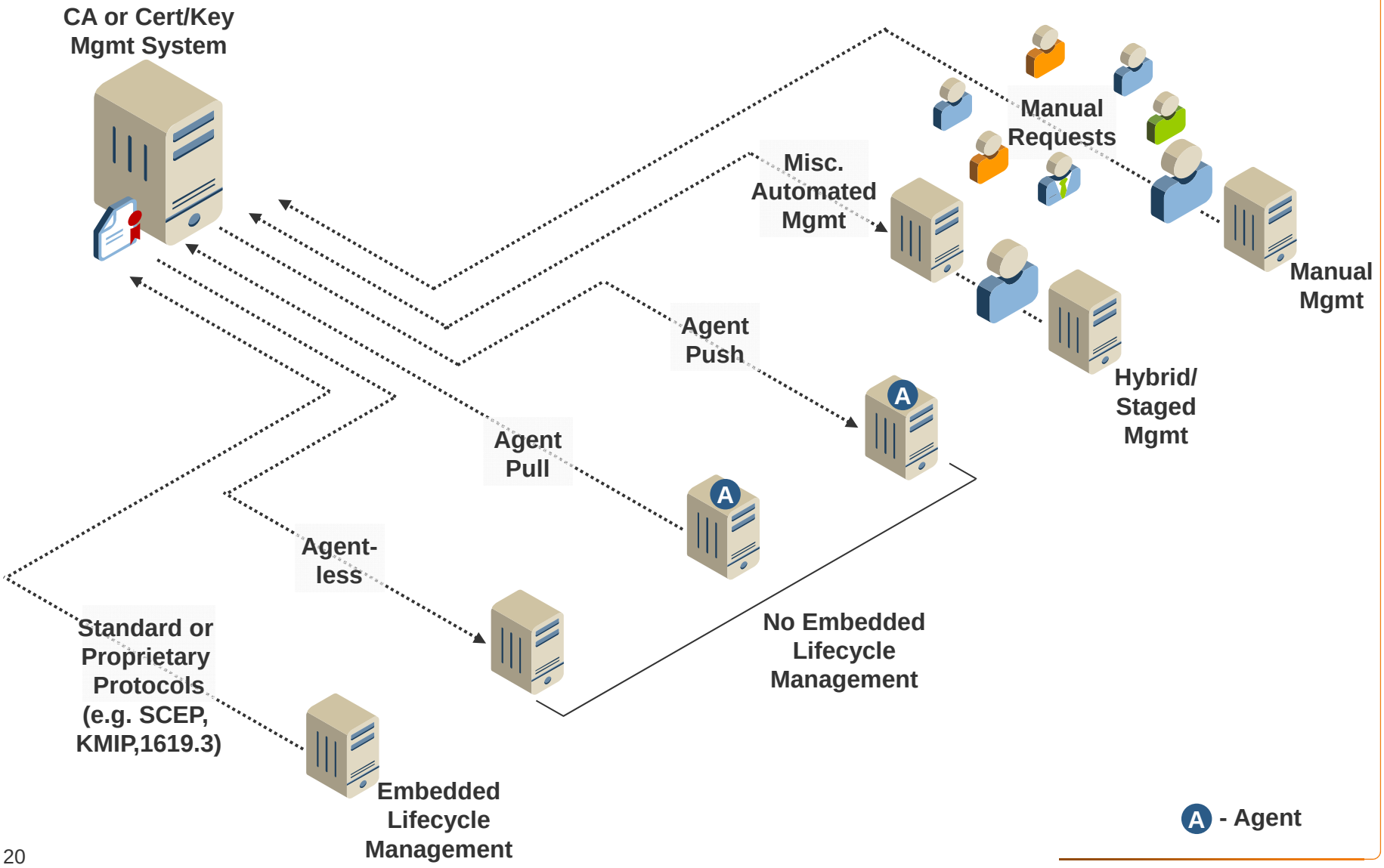
Preparing for and Responding to CA Compromise

1. Establish an accurate inventory of certificates
   - Identify Owners
2. Ensure only trusted CAs are in use
3. Review CA security
4. Establish backup CA(s)
5. Inventory trust anchors (root certs)
6. Create strategy for rapid certificate replacement (to minimize business interruptions due to CA compromise)
7. Establish method of tracking replacement of certificates

Discussion

VENAFI™

Encryption Management and Distribution Models



Another Risk: Private Key Security