Filename: microsoft-server70742-4-2-5-manage-certificates-pt5
Show Name: Identity with Windows Server 2016 (70-742)
Topic Name: Implement Active Directory Certificate Services
Episode Name: Manage Certificates Pt 5
Description: In this episode, Aubri and Mike continue to set up key archival. They issue a certificate that includes key archival. Then they demonstrate going through the process of key recovery.

4.2 Manage Certificates Pt 5

- Configure and manage key archival and recovery

```
Configure Key Archival
  Configure Key Recovery Agent certificate template
    - Create kra account
    - Duplicate Key Recovery Agent template
    - Grant enroll permission to corp\kra
    - Configure CA to issue certificate
    - Log in as KRA and request Key Recovery Agent certificate
    - Approve certificate for issue
    - Configure Recovery Agents on CA properties
      - Choose # of recovery agents
      - Add recovery agent certificate
      - Restart AD CS
    - Configure new template to include key archival
      - Duplicate ITProTV Computer
      - Archive subject's private key
      - Supersede previous ITProTV computer certificate
      - Right-click original template and reenroll all certificate holders
    - In certsrv console, add Archived Key column and wait
```

```
Perform Key Recovery
  - Find Certificate in issued certificates
  - Properties -> Details -> Serial Number
  - Copy and remove spaces
  - certutil -getkey <serialNumber> c:\<path>\outputblob
  - certutil -recoverkey c:\<path>\outputblob c:\<path>name.pfx
  - User can then import .pfx
```