SCEP

Simple Certificate Enrollment Protocol

Widely Deployed

- Cisco routers, VPN client, and CA
- Microsoft CA
- Entrust CA
- RSA toolkit and CA
- Netscape CA
- Verisign CA
- Baltimore/Unicert

Features

- Initial Enrollment
- Renewal (including client key rollover)
- CA and Client Certificate retrieval
- CA key and certificate rollover
- Extensible

Mature Protocol

- Has Been in use for over 7 years
- many interoperable implementations
- Now on draft 15

Enrollment

- PKCS-10 to specify what should be in the cert
- Signed and Encrypted with PKCS-7
- Can Use One-Time Password for authentication

Renewal

- Signed by prior client certificate

CA Key Rollover

- “Next” CA Certificate generated ahead of time
- Clients Can Retrieve “Next” CA Certificate
- Response is signed by current CA certificate
- Roll Over when Old Certificate Expires
- Can roll over “early” if Root CA compromised

Current draft

- **draft-nourse-scep-15.txt**
- **Informational**
- **nourse@cisco.com**