Stephen Farrell
(stephen.farrell@sse.ie)

General

- **Operations:**
  - Registration
  - Certification
  - Key Update
  - Certificate Update
  - Revocation
  - Cross Certification
  - ...?
- **Flexibility:**
  - who generates keys
  - who publishes keys
  - who initiates operations
  - different publishing methods
    - mail, IP, X.500, HTML
  - different cryptotokens

Stephen Farrell
(stephen.farrell@sse.ie)

CA Key Update Requirements

- No effect on other key pairs
- Valid certificates stay valid
- End entities with the old CA public key to be able to verify certificates protected with the new
- Entities not certified by "this" CA should be able to trust it's new & old certificates

Stephen Farrell
(stephen.farrell@sse.ie)

A Scheme

- Idea is to publish new key protected using old, ... and vice versa
- CALinkage data structure is defined in the I-D
- CA must publish these structures when it updates
- Procedure for certificate verification also given

Stephen Farrell
(stephen.farrell@sse.ie)

Example

- Certificate signed with new private key
- Verifier has local (trusted) copy of old CA public key
- Verifier must access CALinkage structure to get a trustworthy copy of the new public key
- Other cases are given in the draft

Stephen Farrell
(stephen.farrell@sse.ie)

Old Private Keys

- Some applications (e.g. mail) impose a requirement that old private keys be accessible for decryption
- Often there is not enough local storage for these (e.g. smartcard)
- It is possible to build this in to the key update procedures (if enough applications require it)