Stephen Farrell
(stephen.farrell@sse.ie)

Local Registration Authority

- Many situations call for the existence of more than just CAs and end entities
- Needed in most cases where the end entity is part of an organisation
- Different terms exist:
  - Local Registration Authority
  - Organisation RA
  - Merchant RA
  - all the same thing

Software and Systems Engineering Limited
A Siemens Company

Stephen Farrell
(stephen.farrell@sse.ie)

Reasons for an LRA

- Token initialisation
- Key Generation
- Pubishing certificates
- Re-issuing credentials
- Revocation requests
- Reduce the number of CAs

Software and Systems Engineering Limited
A Siemens Company

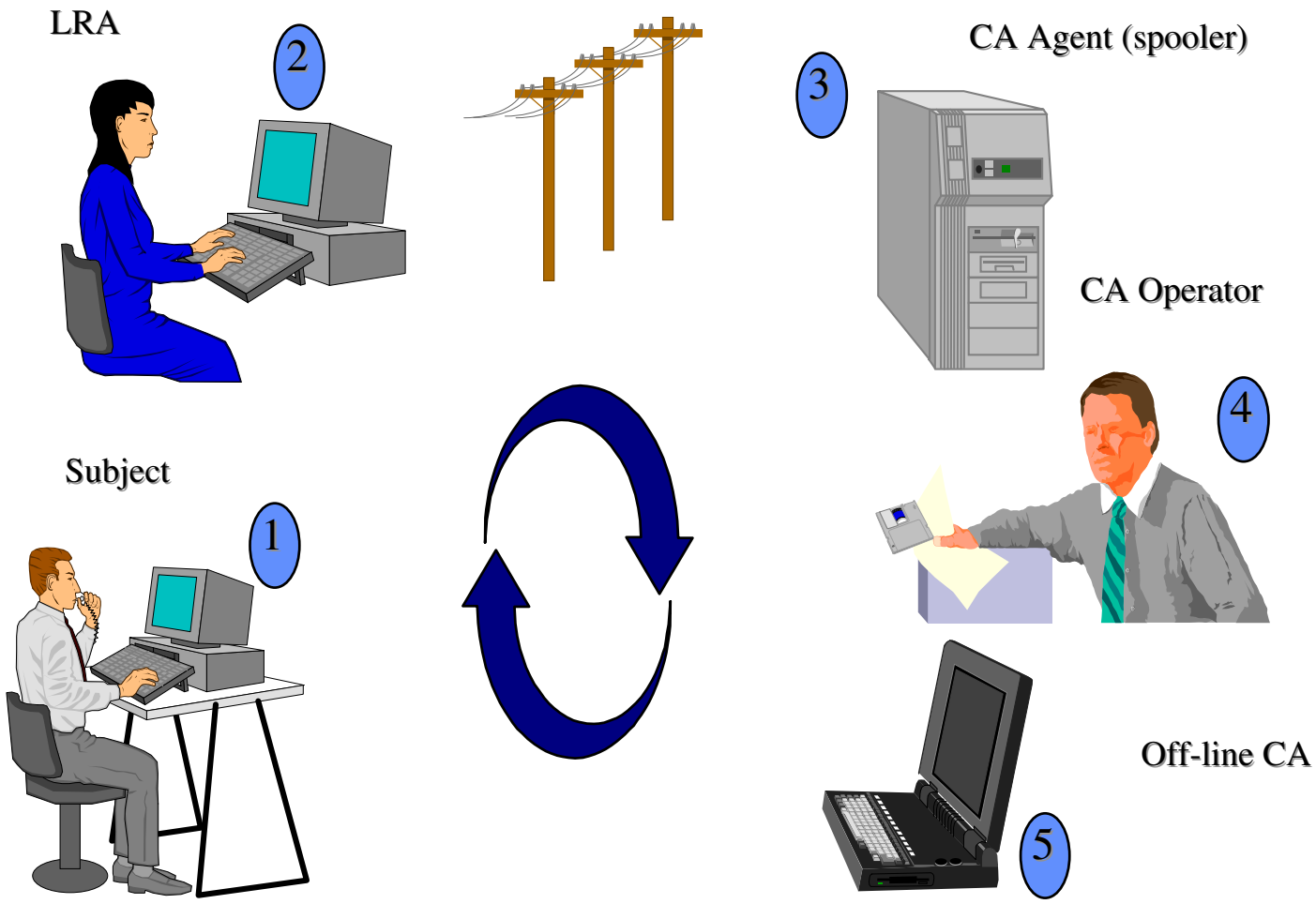
Stephen Farrell
(stephen.farrell@sse.ie)

More reasons

- End users shouldn't have to know about X.509
- Identifying people
- Managing applications
- Organisational Structure
- Tie-in to other registration requirements
- Obvious candidates exist

Stephen Farrell
(stephen.farrell@sse.ie)

PKI with an LRA



Software and Systems Engineering Limited
A Siemens Company

Stephen Farrell
(stephen.farrell@sse.ie)

LRA operation

- One possibilty for initial certification:
  - LRA verifies identity of individual
  - LRA generates key pair
  - LRA sends certification request to CA
  - LRA receives Certificate from CA
  - LRA publishes Certificate
  - LRA issues private key + certificate + CA public key to individual
- This one covers most cases

Stephen Farrell
(stephen.farrell@sse.ie)

Conclusion

- Have to allow for cases where there are three named parties in the management protocols
  - i.e. CA, subject, LRA
- More options exist
  - e.g. for who generates keys
  - should be “pruned” to make interop. simpler
- LRA is a commercial necessity!