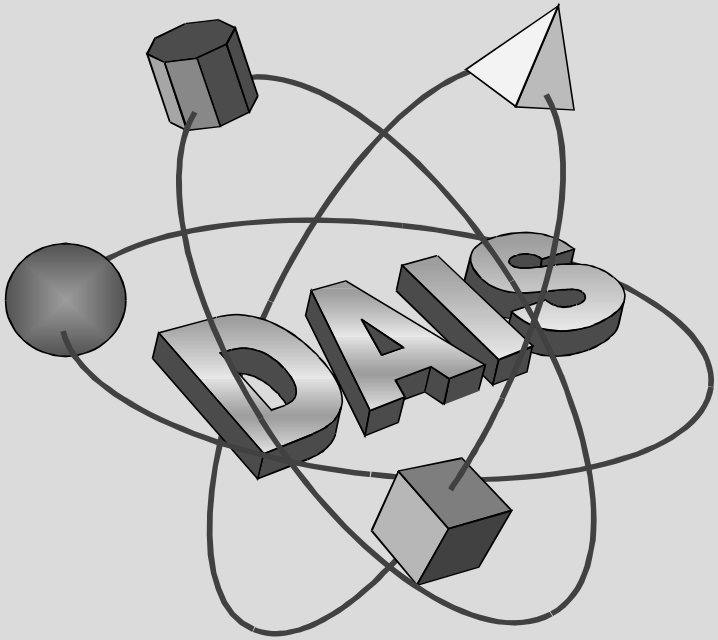


CORBA Security in DAIS

Belinda Fairthorne, ICL

belinda@iclnet.co.uk

DAIS

- DAIS 3.1 conforms to the CORBA 2.0 standard
  - URL: http://www.icl.com/dais
- DAIS 3.1 has beta release of DAIS Security
  - most of CORBASEC level 2 including
    - authentication, secure invocations, auditing
    - privilege based access control including role & identity
    - domain based security policy administration
  - security replacability interfaces
    - Vault, Security Context, Access Decision etc

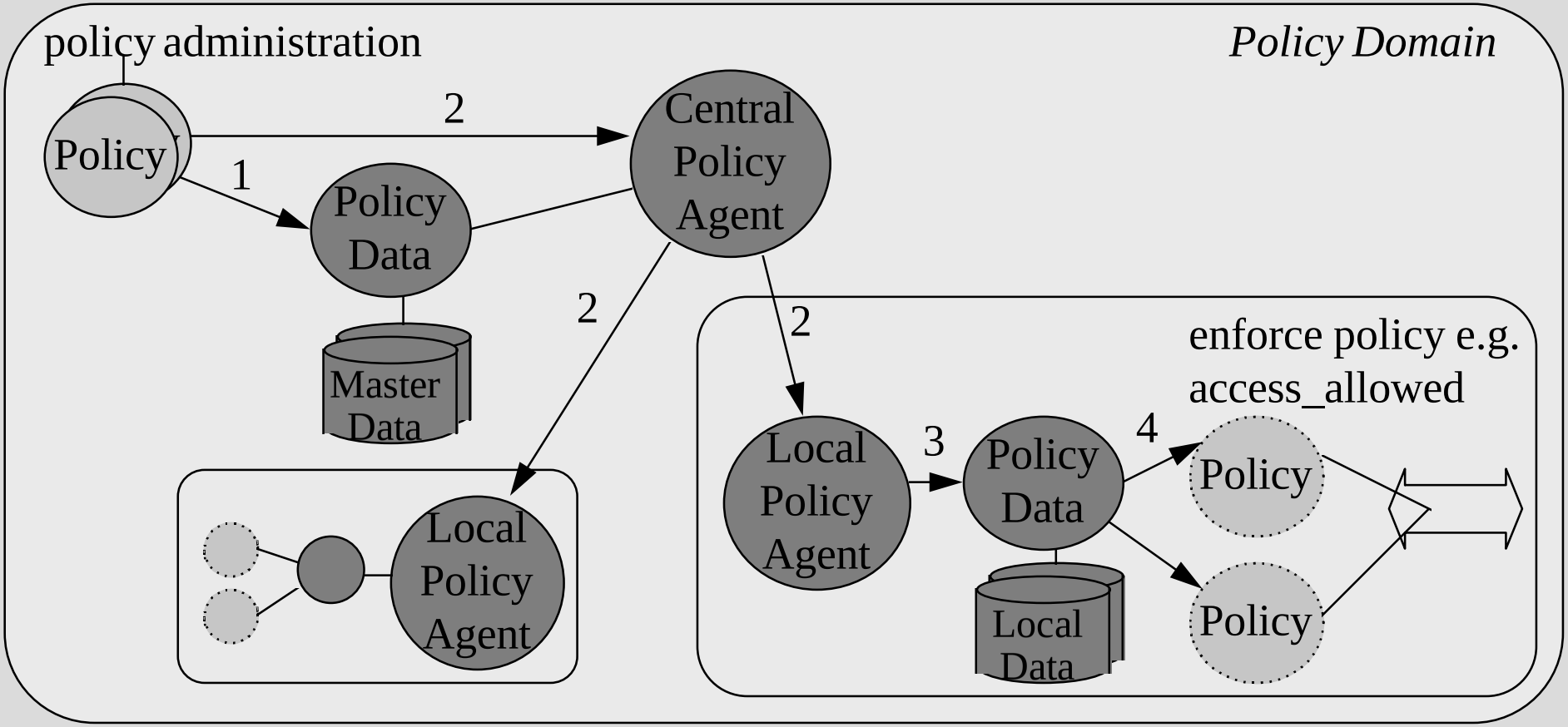
Some Implementation Points

- Security policy administration
  - using domain policies and replacability interfaces
  - with performance in mind
- Use of security services replacability interfaces
  - with different security mechanisms
- Object interfaces to Certificate Management
  - Certification Authority etc

Security Policy Administration

- DAIS implements domain based administration for
  - CORBASEC policies e.g. AccessPolicy, AuditPolicy
    - DomainAccessPolicy supports role etc based access controls
  - required rights
  - security mechanism policy
- Domains can span nodes of network
  - can also have multiple domains at one node
- Central Policy administration per domain
  - Policy Agents distribute policy information
    - for all policy types
  - Policy (pseudo-)objects use cached policy information
    - for fast policy enforcement

Policy Objects

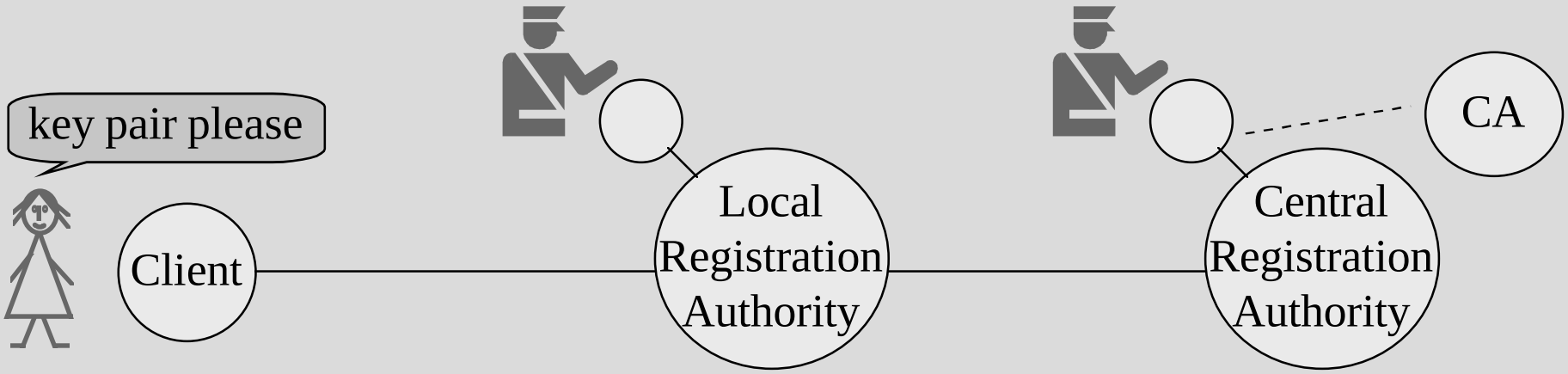


1. initial policy changes
2. propagate changes to Local Policy Agents
3. update local policy data
4. re-read updated data

Security Replacability

- DAIS implements Security Services replacability
  - and uses GSS-API within Vault, Security Context objects
- Uses CSI_ECMA (SESAME) to provide
  - roles and other privileges for access control
  - public key technology
  - also support secret & hybrid key options as in CSI_ECMA
- DAIS was implemented with Kerberos first
  - Replaced Kerberos by SESAME using GSS-API interfaces
    - easily

Object based Certificate Management



- User requests private/public key pair
- Local registration authority (LRA) generates keys
  - according to local rules enforced by local registration officer
- Certification Authority generates certificate
  - according to rules enforced by central registration officer
  - CA may be on-line or off-line, depending on policy
- Certificates can be revoked by user, LR officer or CR officer
- Certificates and keys held by and used by security services