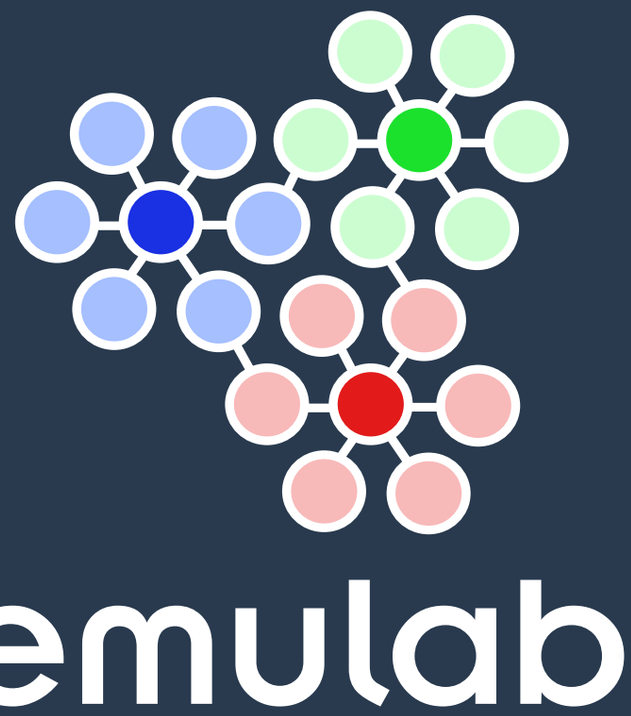
ProtoGENI Security Model

Robert Ricci, GEC #4
April 1, 2009



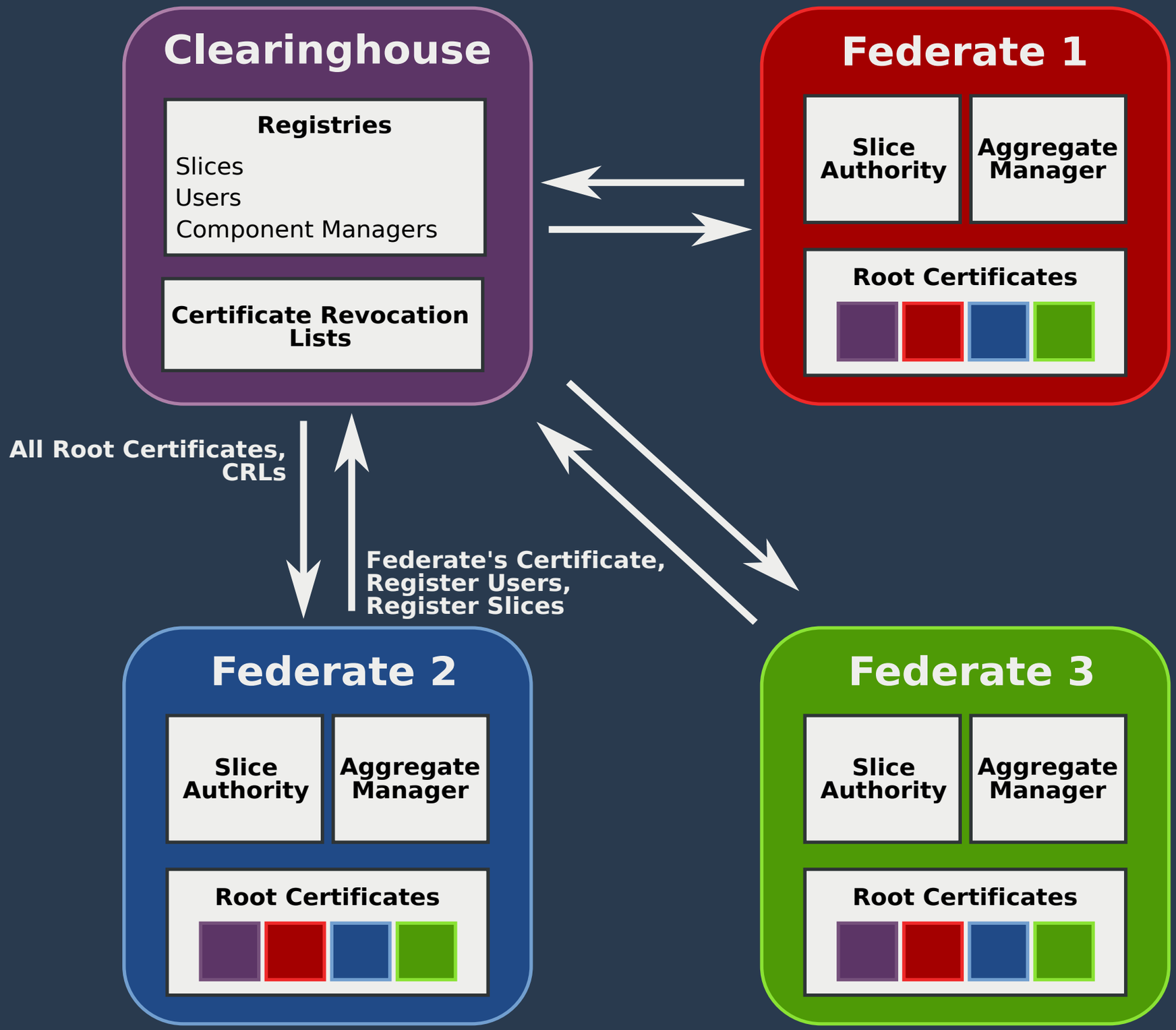
Principles

- Simple model now
  - High degree of trust
  - Flat trust structure
- Design supports more complicated models later
  - Trust is not a full graph
  - Hierarchical federation structure
- All parties trust clearinghouse
- Authorization is attribute-based (credentials)
- Use standard technologies

"PKI"

- Extremely simple
- Each federate is a CA
- "Browser model" - everyone shares a CA set
- Clearinghouse used as central point for root certs and CRLs

Certificate Exchange



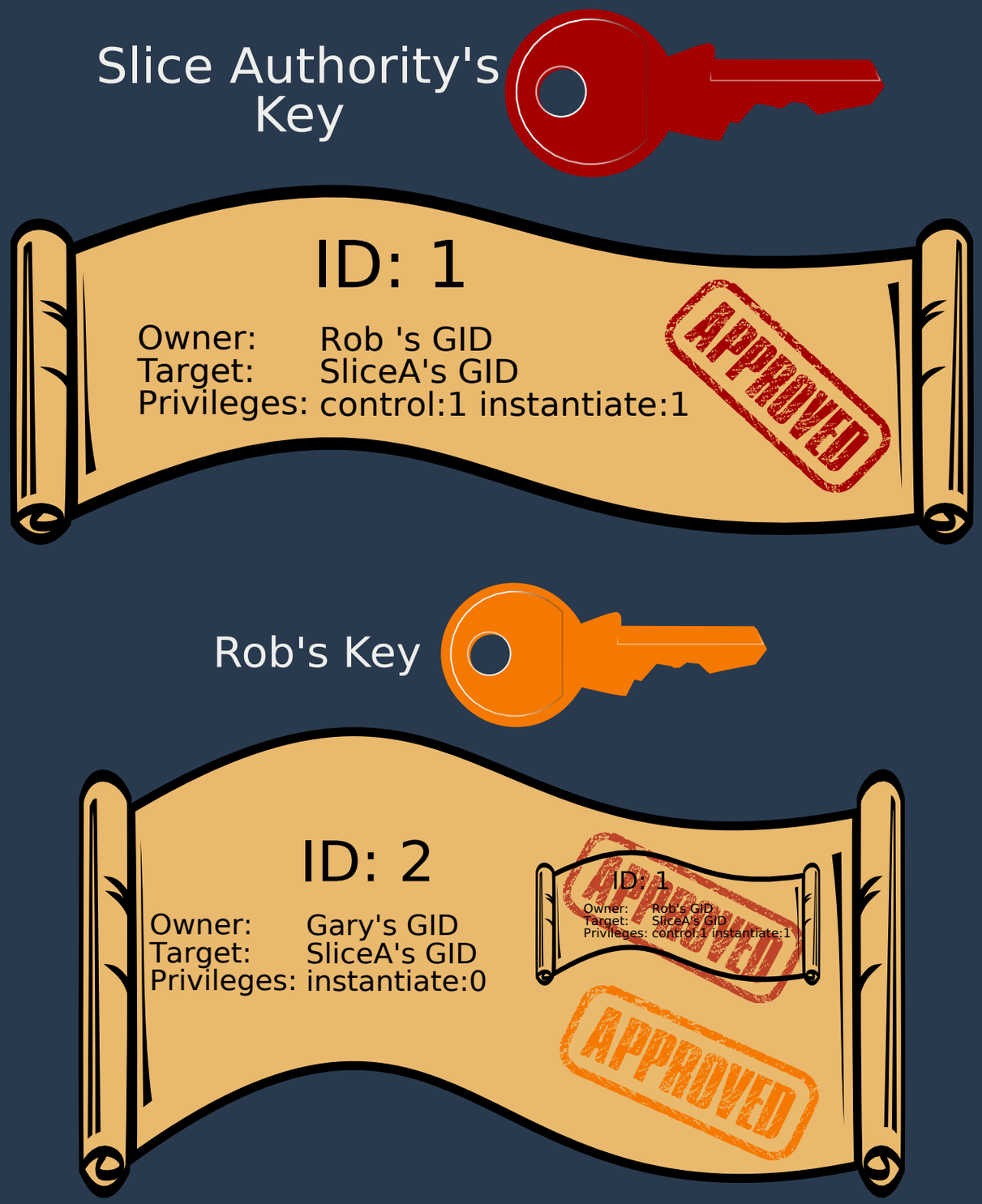
Authenticating Users

- SA signs user certs
- Today: Check signature against root certificate set
- Soon: Chains for hierarchical SAs
  - Client cert includes all higher-level certs
- Check against periodically-downloaded CRL

Authorizing Users: Credentials

- Bound to a specific principal
- Includes
  - Unique ID
  - Owner GID
  - Target GID
  - Set of privs
- Signed by target's authority

- Delegation
  - Includes initial credential
  - Possibly subset of privileges
  - Signed by owner's key



Big Remaining Issues

- GID contents and semantics
  - Self certification vs.
  - Separation of identity and authentication
- Protecting against malicious or buggy authorities
- Trial of hierarchical trust
- Authorization that crosses the hierarchy

end