CoreGRID

CCLRC
Rutherford Appleton Laboratory

GridTrust

Trust and Security in Grids

Alvaro Arenas

E-Science Centre

Bridging Global Computing with Grids – November 2006

Outline

- Grid Concepts
- Grid Security Today
- Secure Virtual Organisation Management
- Next Generation Grids
- Trust and Security Challenges in NGG
- Facing the Challenges

Acknowledgments

Ideas presented here are result of discussions with colleagues and friends from other projects. In particular,

- TrustCoM
  - Theo Dimitrakos, BT
  - Michael Wilson, CCLRC
- CoreGRID
  - Keith Jeffery, CCLRC
  - Philippe Massonet, CETIC
  - Syed Naqvi, CoreGRID Fellow
  - Gheorghe Silaghi, CoreGRID Fellow
- GridTrust
  - Juan Bicarregui, CCLRC
  - Brian Matthews, CCLRC

Grids

- Resource sharing and coordinated problem solving in dynamic, multi-institutional virtual organisations (VOs)
  - Large number of unknown and heterogeneous resources
  - Resources and users located in distinct administrative domains
  - Dynamic formation and management of VOs
  - Autonomy
    - Self-configuration, self-healing, self-protection

Grid Security must address …

- Allow for controlled sharing of resources
  - Usually through SLAs
  - Quality of Protection
- Allow for coordination of shared resources
  - Restricted delegation from VO to users, users to resources
- Bridge differences between mechanisms
  - Authentication, policy formats, …
- Establish trust relationships between resources and users

Grid Security Today
Grid Security Infrastructure (GSI)

- VOs for multi-user collaborations
  - Federate through mutually trusted services
- Users able to set up dynamic trust domains
- Based on public-key encryption technology
- Define authentication and authorisation mechanisms that allow collaborating sites to accept credentials while retaining local control
  - Authentication using a single-sign-on mechanism
- Each user has a Grid id, a private key, and a certificate signed by a Certification Authority

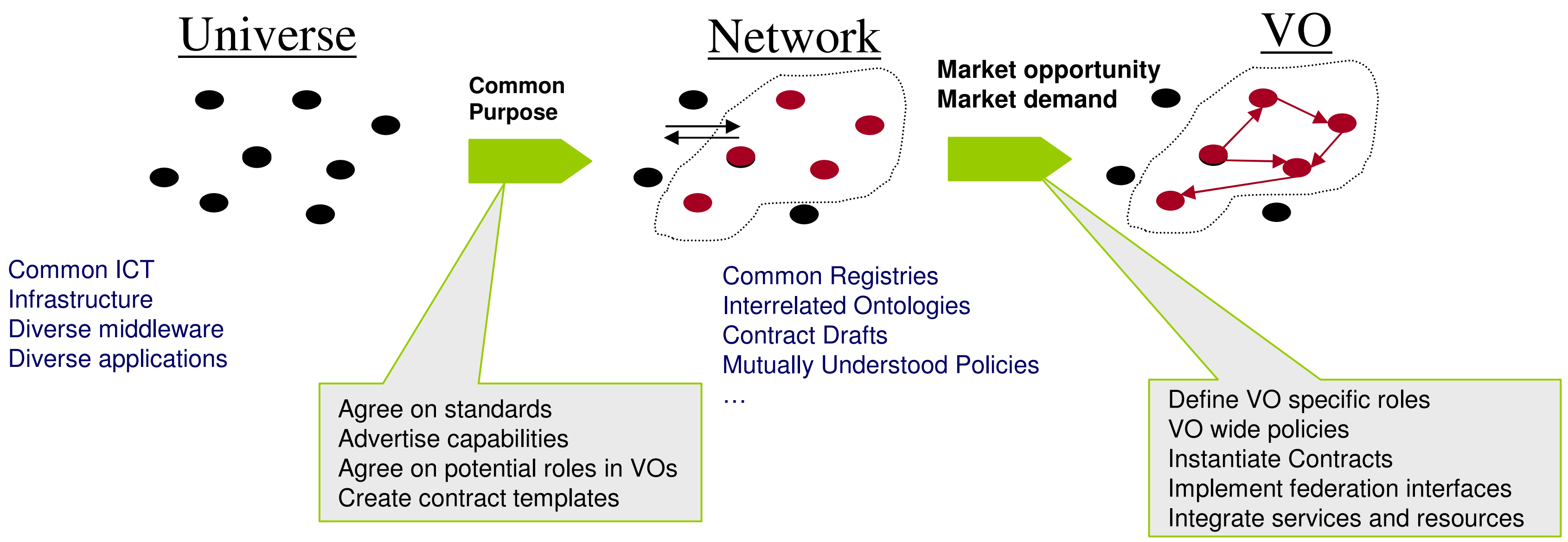
Advantages and Drawbacks

- Advantages
  - Based on standards: X.509, SSL/TLS, …
  - Widely used implementations (e.g. CAS, VOMS), although mainly by the e-Science community

- Drawbacks
  - Traditional access control does not scale up well
  - Mainly static policies; no checking on policy conflicts
  - Basic support for delegation
  - Lack of “soft security” – social control mechanisms such as reputation

Bringing the VO Lifecycle of Virtual Enterprises into Grids

- Developed by the TrustCoM Project



Universe

Common Purpose

Network

Market opportunity
Market demand

VO

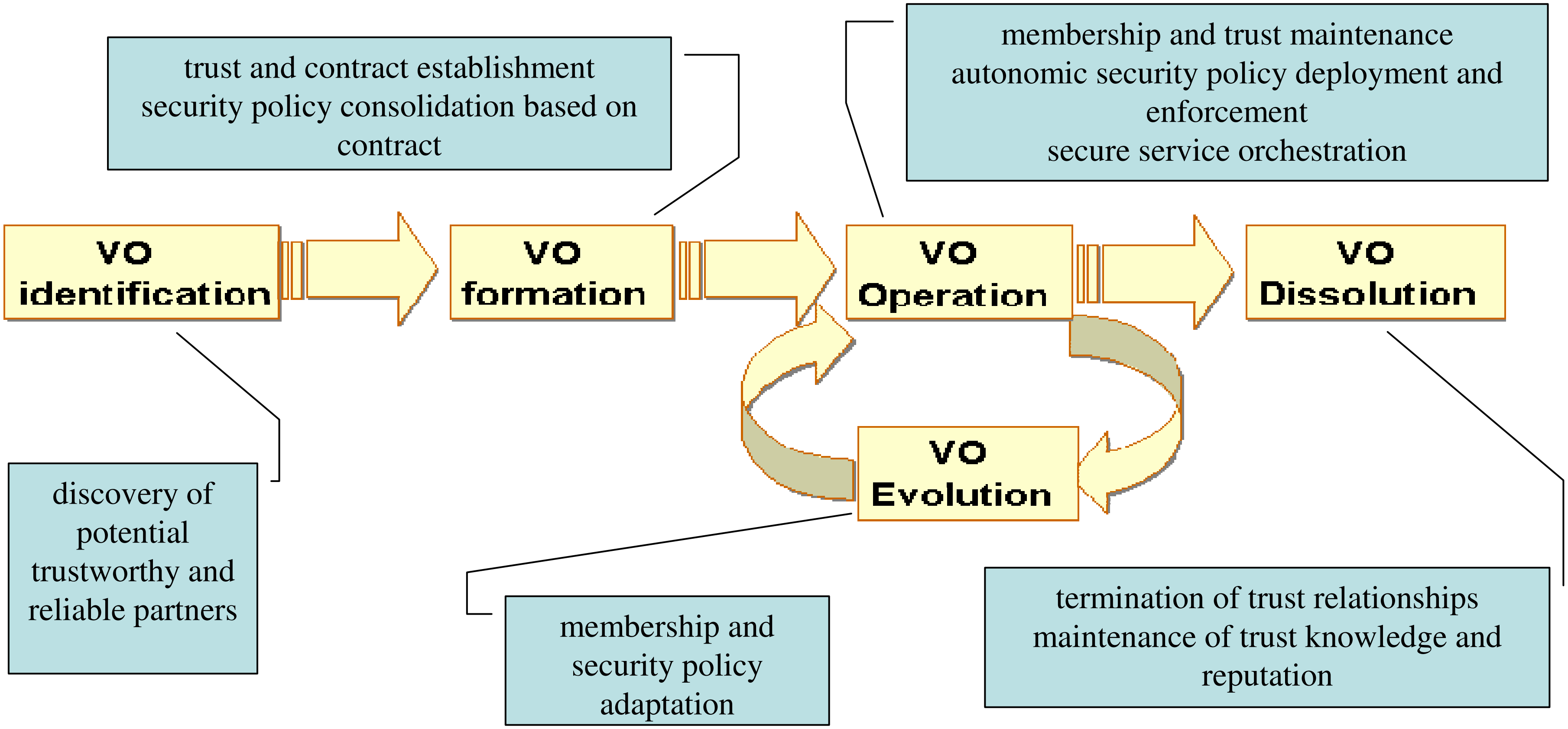
Common ICT
Infrastructure
Diverse middleware
Diverse applications

Agree on standards
Advertise capabilities
Agree on potential roles in VOs
Create contract templates

Common Registries
Interrelated Ontologies
Contract Drafts
Mutually Understood Policies
…

Define VO specific roles
VO wide policies
Instantiate Contracts
Implement federation interfaces
Integrate services and resources

Secure VO Management



VO identification

discovery of potential trustworthy and reliable partners

VO formation

trust and contract establishment
security policy consolidation based on contract

VO Operation

membership and trust maintenance
autonomic security policy deployment and enforcement
secure service orchestration

VO Evolution

membership and security policy adaptation

VO Dissolution

termination of trust relationships
maintenance of trust knowledge and reputation

Next Generation Grids

- Service-Oriented Knowledge Utility (SOKU)
  - Service-oriented architecture
  - Services are knowledge assisted
  - A utility is a service with standardised functionality, emphasising trust, dependability and security
  - A way of building, operating and evolving IT intensive solutions
  - Enables the use of services with the same dependability, safety, and ubiquity as existing utilities such as power or water

Trust and Security Challenges

- Dynamic Composition of Services
  - How the integrity of security is maintained such that the final composition is consistent when services are discovered / composed automatically
  - What is the certification of "fitness for purpose" – functional and non-functional (trust/security, privacy, performance, …)
- Multi-domain environments with entities having multiple identities and roles
  - New forms of identity management
  - Safe digital signatures using advanced techniques (quantum computing)
- Virtualisation in Security
  - Security services that can provide complete abstraction of their underlying technology
  - Configurable security services

Trust and Security Challenges

- Scaling of Authorisation Schemes
  - Require local identification, authorisation and generation of trust credentials
  - Who guards the guards – How does one “police” the guys setting the credentials and running the certification systems
- Trust
  - What it means to trust a service/agent/workflow
  - How to trust an entity which is not under direct control
  - Virtualisation vs Trust
- Trust Management
  - Interplay between trust and reputation in Grids (soft security)
  - Distributed trust management systems
  - Privacy issues in trust management

Trust and Security Challenges

- Information Flow in Grids
  - Languages for describing security requirements, policies at several levels (VOs, users, resources), information and data
  - Negotiation of security credentials, policies, trust
- Nomadic Grids – Mobility
  - Future grid users will prefer to access the resources from small devices
  - A grid security architecture should be capable of providing complete set of security services to these users

Facing the Challenges
Bringing GC into Grids

- Conceptual frameworks for predictable operation under uncertainty
  - Logics and tools to reason about security across different domains, resources and their interaction

- Sustainable Security
  - Systems evolve: new pattern of usage, new threads
  - Methods for sustain security