Facilitating Flexible and Versatile Centrally Administered Community of Interest Organization and Control

Kevin Foltz, Coimbatore Chandersekaran

Institute for Defense Analyses
Alexandria, VA, USA
{kfoltz | cchander}@ida.org

Agenda

- Introduction to COIs
- Prior Work
- New Contributions

Introduction to Computer Collaboration

- Goal: several people work together and share resources
  - Temporary joining of entities for goal-oriented task
  - Limited trust
  - Limited resource sharing
  - Different types of organizations
  - Parts of organizations involved

Scenario

- Objective: Find terrorist leader known to be hiding in Eastern Europe
- Collaborators: Selected officials from law enforcement and intelligence agencies in U.S and select E. European countries (e.g. Poland, Ukraine, Belarus), as well as European-wide agencies such as Interpol

- Operation Requirements:
  - Collaborators gather data through human and electronic means (i.e. sensors) and combine to analyze information to pinpoint terrorist's whereabouts.
  - Mission is time-sensitive—collaboration must begin quickly
  - Officials will continue to work for their original organizations

- Nature of Collaboration:
  - Intelligence agencies share information learned from regional agents
  - Law enforcement agencies make available portions of criminal database, enlist local law enforcement when needed
  - Electronic intelligence shared among all parties
  - Intelligence agencies given limited freedom in all participating nations

Scenario

- Security Requirements
  - Information provided is extremely sensitive
  - Interactions must be strongly authenticated
  - All actions in collaboration fully audited
  - All collected data is confined to the collaborator community
  - Parties are distrustful of one another
  - Collaborators may not share all data collected in pursuing objective

Simple Solutions

	Share files	Version Control
Email Files	Y	N

Simple Solutions

	Share files	Version Control	Finding Resources
Email Files	Y	N	
Servers Hold Resources	Y	Y	N

Simple Solutions

	Share files	Version Control	Finding Resources	Access Control
Email Files	Y	N		
Servers Hold Resources	Y	Y	N	
Discovery Service	Y	Y	Y	N

Simple Solutions

	Share files	Version Control	Finding Resources	Access Control	Authentication
Email Files	Y	N			
Servers Hold Resources	Y	Y	N		
Discovery Service	Y	Y	Y	N	
Membership	Y	Y	Y	Y	N

Simple Solutions

	Share files	Version Control	Finding Resources	Access Control	Authentication	Authorization
Email Files	Y	N				
Servers Hold Resources	Y	Y	N			
Discovery Service	Y	Y	Y	N		
Membership	Y	Y	Y	Y	N	
Credential-based naming/authentication	Y	Y	Y	Y	Y	N

Simple Solutions

	Share files	Version Control	Finding Resources	Access Control	Authentication	Authorization	Collaboration Rules
Email Files	Y	N					
Servers Hold Resources	Y	Y	N				
Discovery Service	Y	Y	Y	N			
Membership	Y	Y	Y	Y	N		
Credential-based naming/authentication	Y	Y	Y	Y	Y	N	
Authorization system	Y	Y	Y	Y	Y	Y	N

Simple Solutions

	Share files	Version Control	Finding Resources	Access Control	Authentication	Authorization	Collaboration Rules	Independent Entity
Email Files	Y	N						
Servers Hold Resources	Y	Y	N					
Discovery Service	Y	Y	Y	N				
Membership	Y	Y	Y	Y	N			
Credential-based naming/authentication	Y	Y	Y	Y	Y	N		
Authorization system	Y	Y	Y	Y	Y	Y	N	
Security policies	Y	Y	Y	Y	Y	Y	Y	N

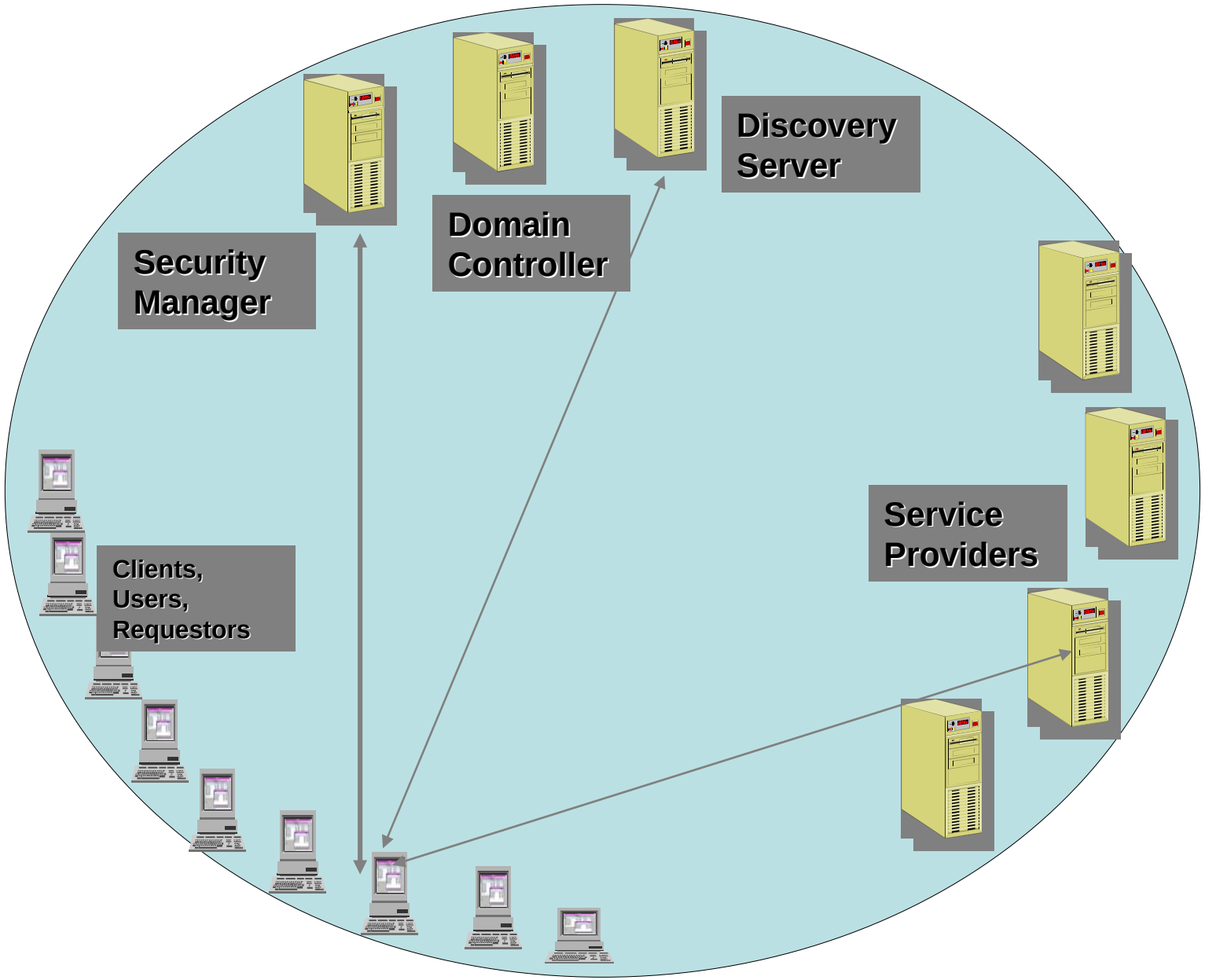
Simple Solutions

	Share files	Version Control	Finding Resources	Access Control	Authentication	Authorization	Collaboration Rules	Independent Entity	Domain Management
Email Files	Y	N							
Servers Hold Resources	Y	Y	N						
Discovery Service	Y	Y	Y	N					
Membership	Y	Y	Y	Y	N				
Credential-based naming/authentication	Y	Y	Y	Y	Y	N			
Authorization system	Y	Y	Y	Y	Y	Y	N		
Security policies	Y	Y	Y	Y	Y	Y	Y	N	
Create domain with users, servers, etc.	Y	Y	Y	Y	Y	Y	Y	Y	N

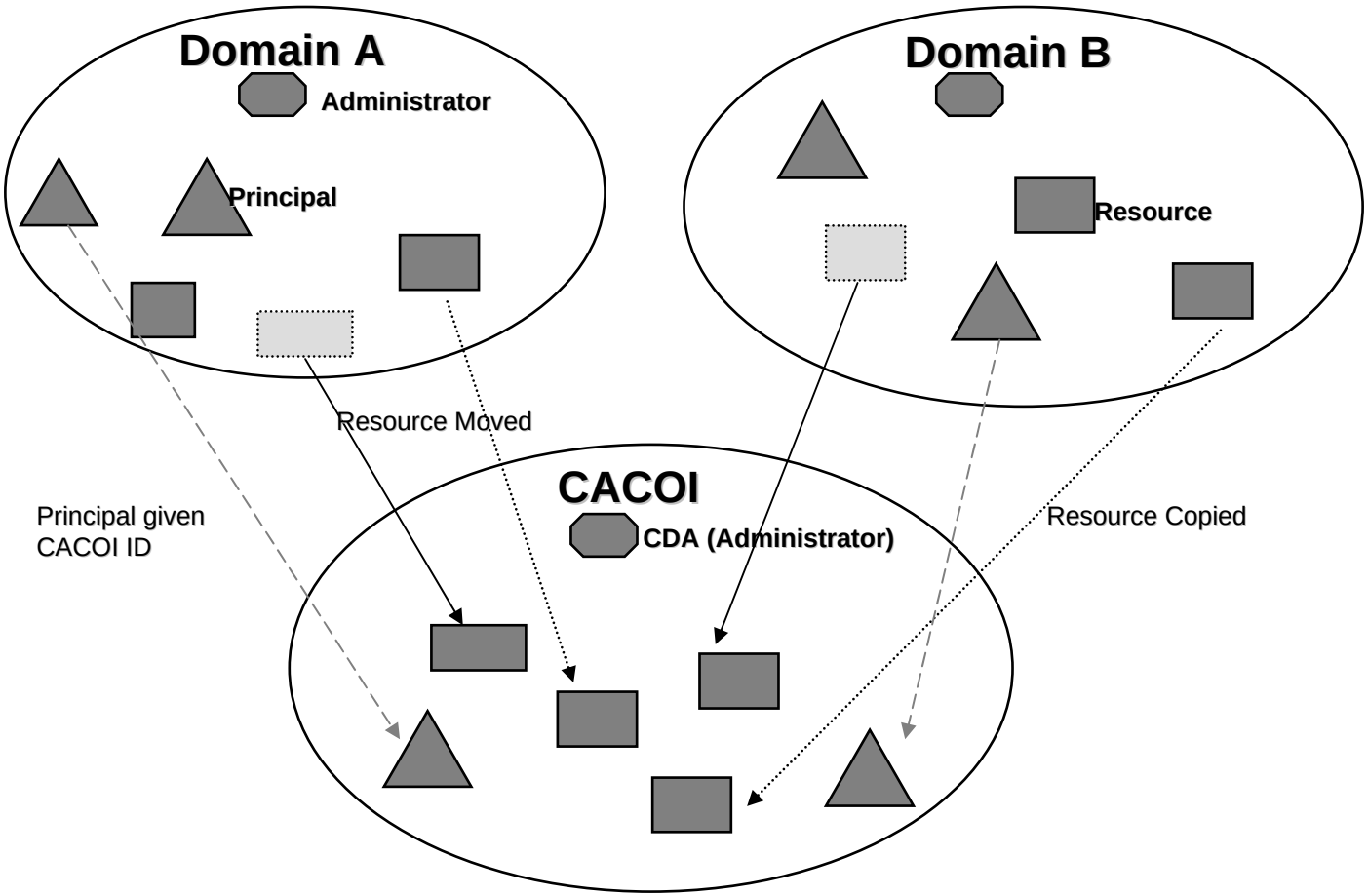
Simple Solutions

	Share files	Version Control	Finding Resources	Access Control	Authentication	Authorization	Collaboration Rules	Independent Entity	Domain Management
Email Files	Y	N							
Servers Hold Resources	Y	Y	N						
Discovery Service	Y	Y	Y	N					
Membership	Y	Y	Y	Y	N				
Credential-based naming/authentication	Y	Y	Y	Y	Y	N			
Authorization system	Y	Y	Y	Y	Y	Y	N		
Security policies	Y	Y	Y	Y	Y	Y	Y	N	
Create domain with users, servers, etc.	Y	Y	Y	Y	Y	Y	Y	Y	N
Domain controller servers and administrator accounts	Y	Y	Y	Y	Y	Y	Y	Y	Y

A Typical Domain



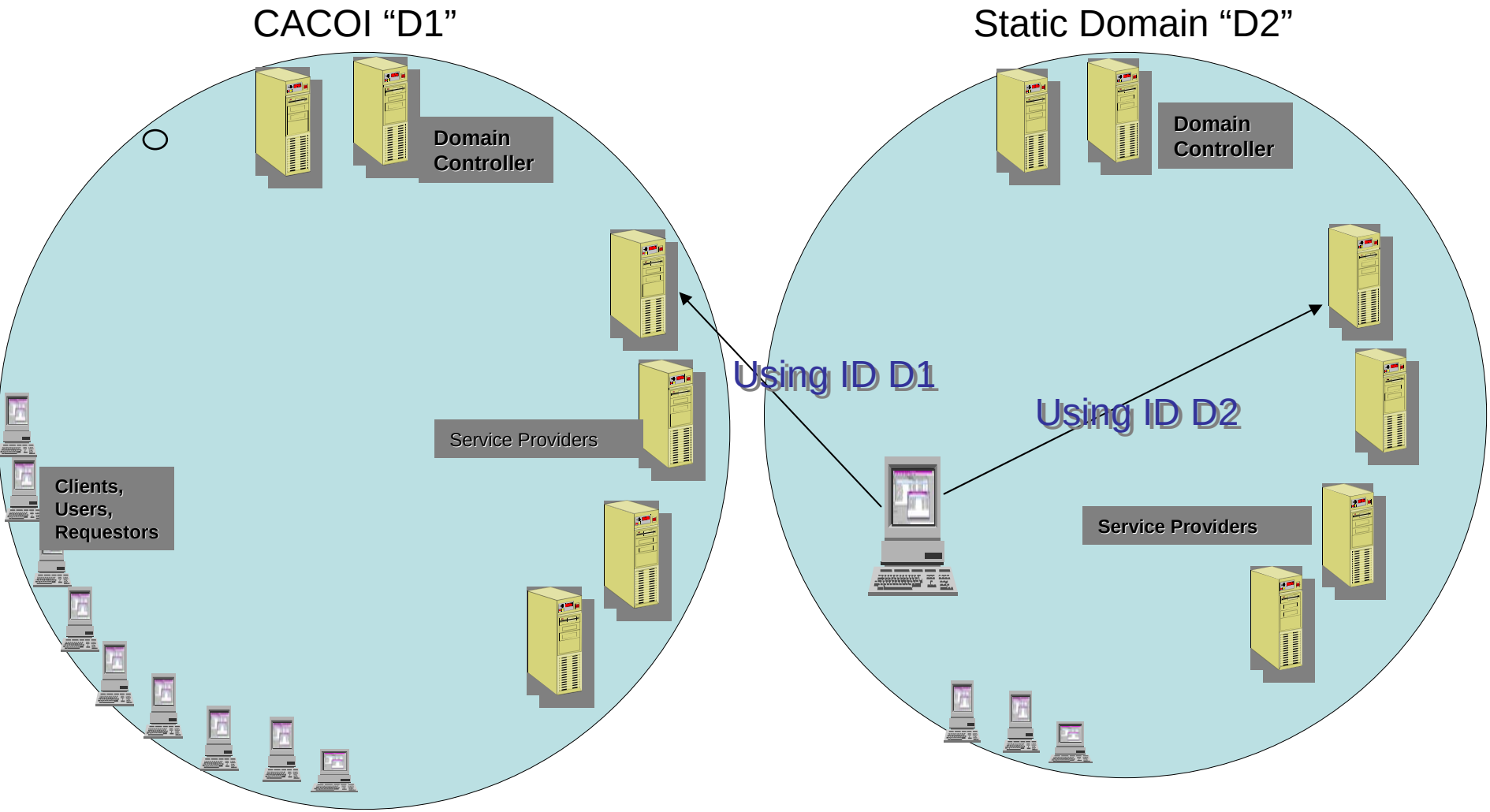
CACOI Basic Structure



CACOI Basic Facts

- All entities are included in one domain
- Users must be logged into the CACOI to access CACOI resources
- All resources in the CACOI are owned by the CACOI
- Resources are either moved or copied to the CACOI
- The fate of CACOI resources is not defined after the CACOI is finished
- Administration is centralized, but group-based administration is possible to allow consensus
- Domain structure based on Microsoft Server 2000 domains and related policies

Usage Model


CACOI “D1”
Static Domain “D2”
Domain Controller
Domain Controller
Service Providers
Service Providers
Clients, Users, Requestors
Using ID D1
Using ID D2

COI Desired Properties

- Rapid assembly/disassembly
- Security policies
- Separate entity
  - Not located within one contributor
  - Not a federation
- Global Data confinement
- Group-based control
- Sharing policies

Prior Studies

	DGSA	P2P	SVE	MDDC	CACOI
• Rapid assembly/disassembly	N	Y	Y	Y	Y
• Security policies	Y	N	Y	Y	Y
• Separate entity	N	N	N	N	Y
• Global data confinement	N	N	N	N	N
• Group-based control	N	N	N	N	Y
• Sharing policies	N	N	N	N	N

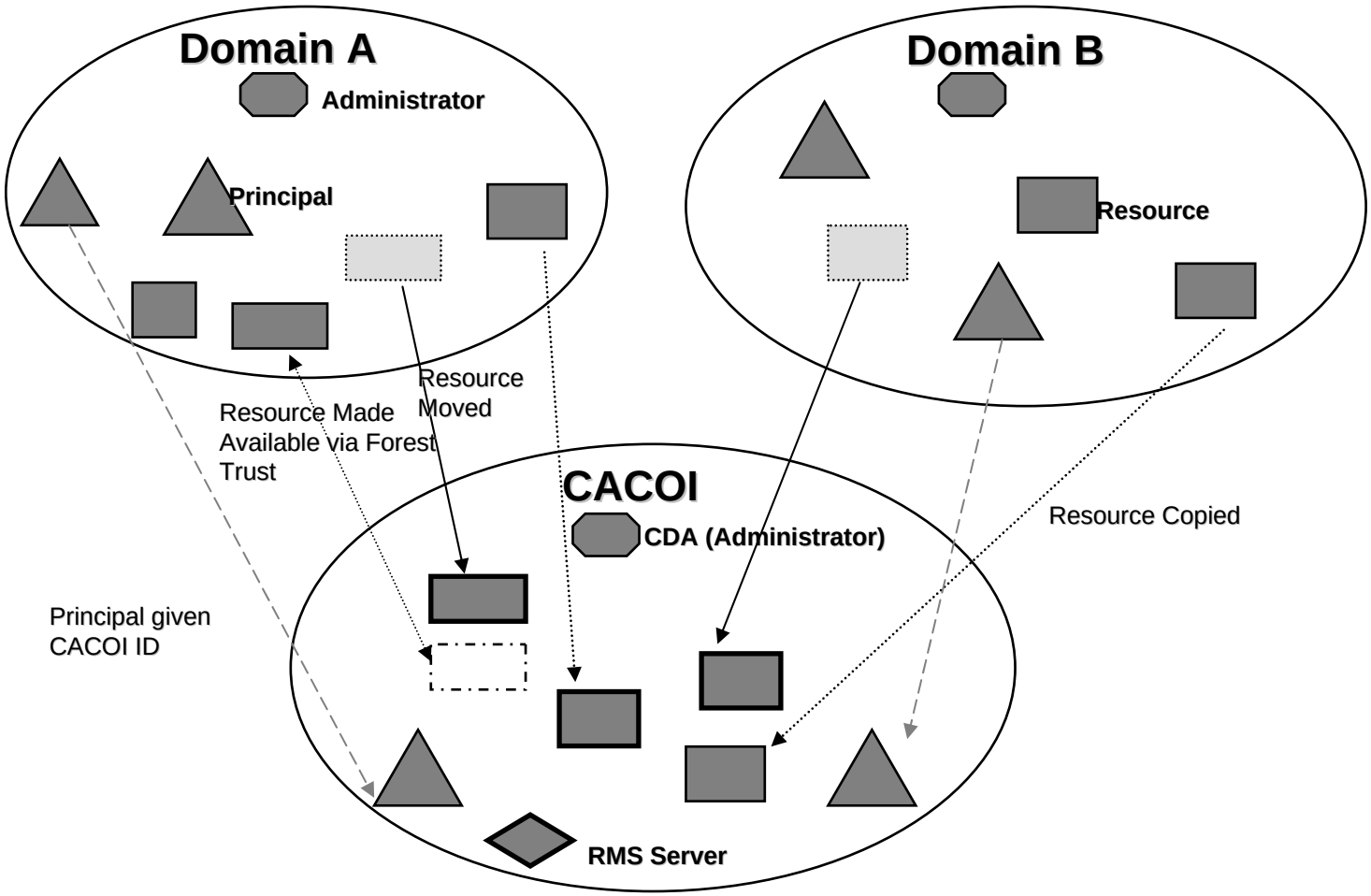
Existing Solutions address some, but not all, goals for COIs

Current Work

	DGSA	P2P	SVE	MDDC	CACOI
• Rapid assembly/disassembly	N	Y	Y	Y	Y
• Security policies	Y	N	Y	Y	Y
• Separate entity	N	N	N	N	Y
• Global data confinement	N	N	N	N	Y
• Group-based control	N	N	N	N	Y
• Sharing policies	N	N	N	N	Y

Current work uses Rights Management to enable global data confinement and trust relationships in Microsoft Server 2003 to enable sharing policies.

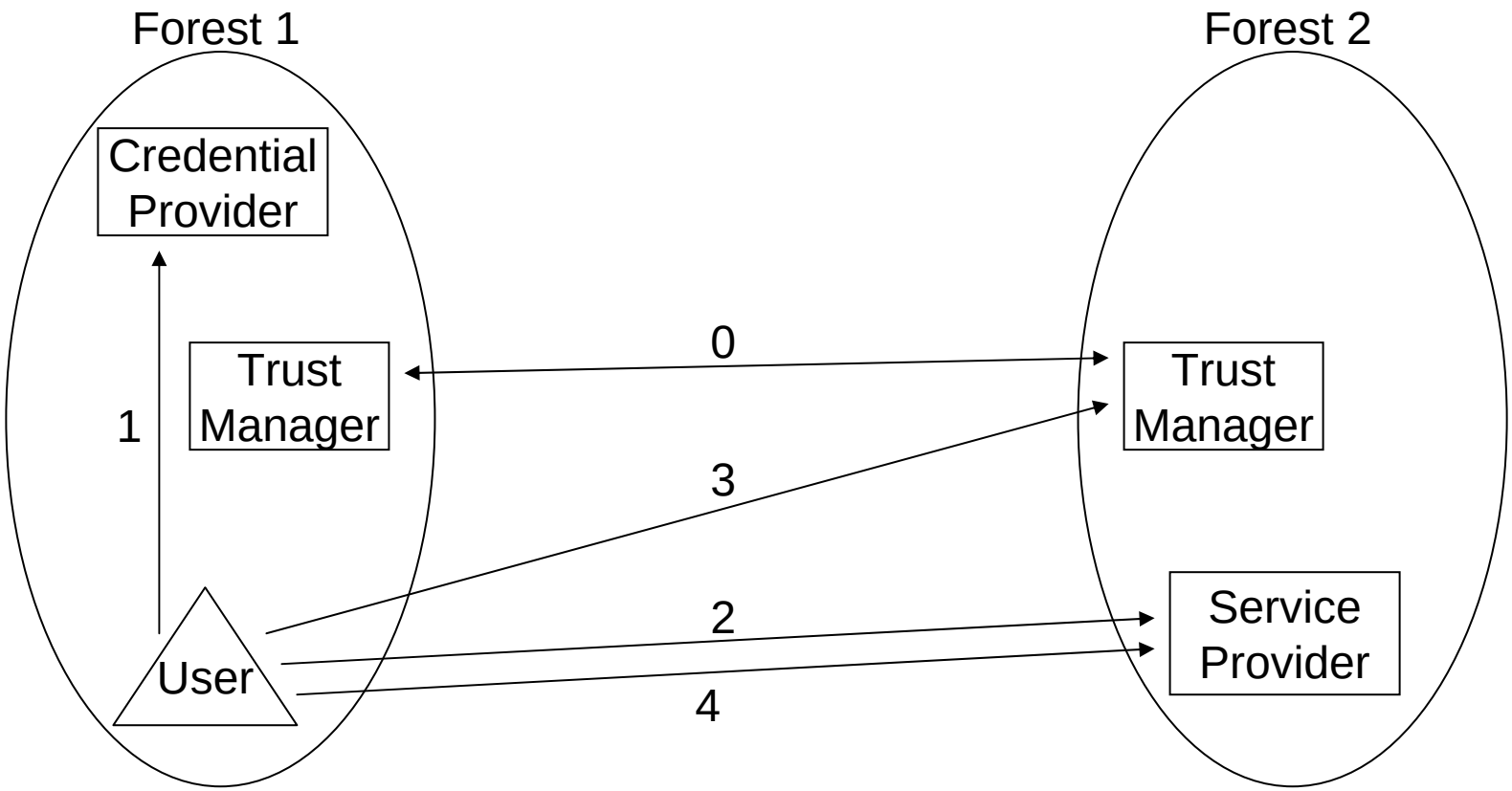
CACOI Enhancements



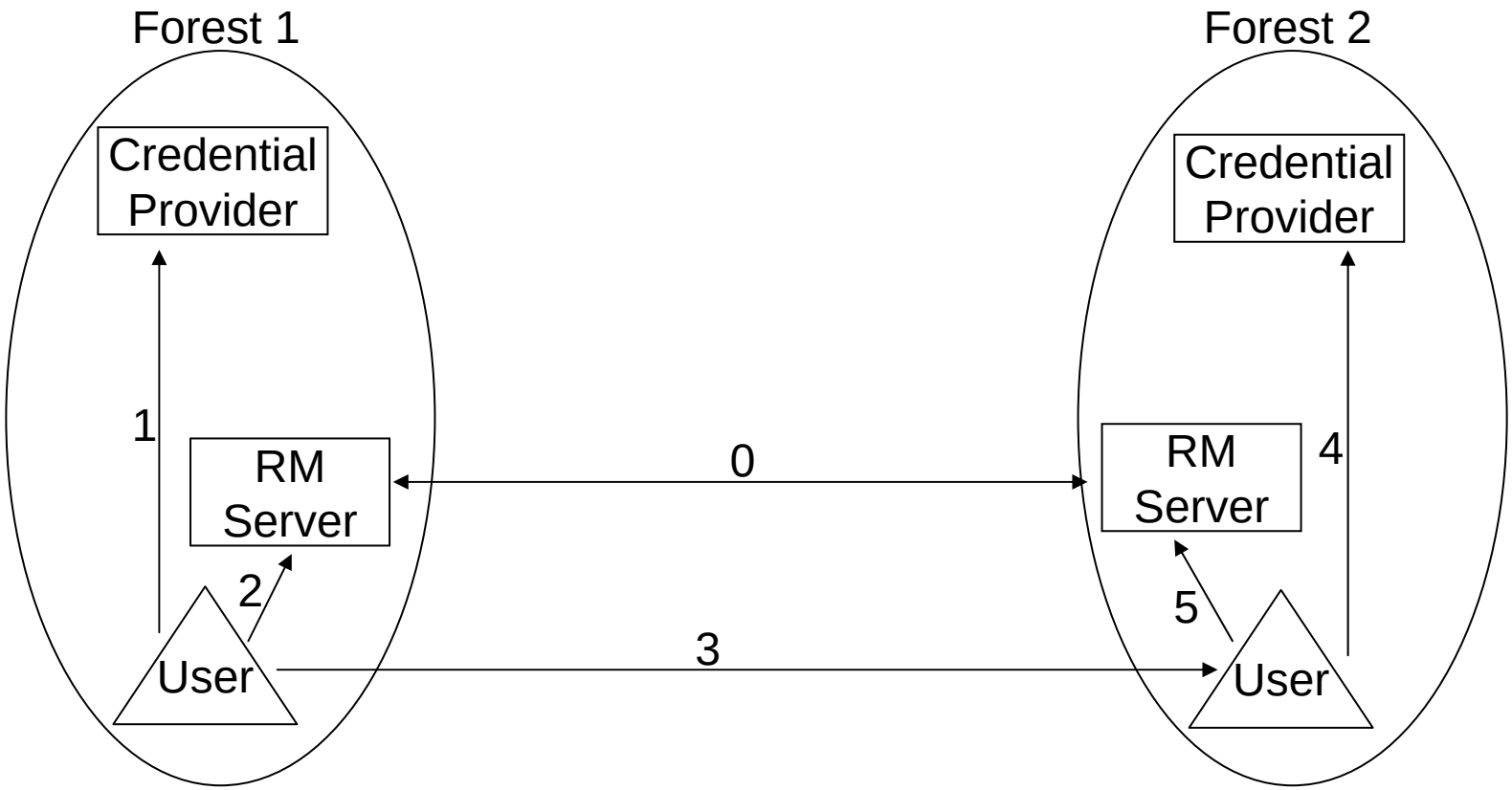
CACOI Enhancements

- Forest Trusts from Microsoft Server 2003
  - Allows remote sharing of resources
  - Gives organizations more control over sharing
- Rights Management Server
  - Allows Digital Rights Management
  - Global confinement

Cross-Forest Trust



Rights Management



Future Work

- Metadata Management
- Operational Issues

Contact Info

Kevin Foltz
Institute for Defense Analyses, ITSD
4850 Mark Center Drive
Alexandria, VA 22311 USA
703-845-6625
kfoltz@ida.org

Sekar Chandersekaran
Institute for Defense Analyses, ITSD
4850 Mark Center Drive
Alexandria, VA 22311 USA
703-845-4399
cchander@ida.org