Enterprise Federation: Essential Research Needed for the GIG

Sekar Chandersekaran AF CIO Office and IDA

Terry Mayfield IDA

August 23 2006

What is the Problem? -1

- Distributed systems
  - Spread across multiple enterprises that need to collaborate tightly to achieve mission objectives
  - Enterprises [within DOD and across Government organizations and other COI 'countries'] are autonomous and make their own choices contributing to heterogeneity
  - Operational environments dictate heterogeneity
    - Tactical Environment and integration
  - Many other factors contributing to heterogeneity
    - Increasing number of protocols
    - Increasingly complex trust relationships
    - Increasing complexity of discovery due to desired 'DYNAMIC BEHAVIOR'
    - Increasing numbers and types of directories
    - Increasing number of content formats and semantics
    - Business needs of commercial products dictate that they distinguish themselves based on specialized capabilities
      - IM across AOL or Microsoft
      - Search Engines [Google, Microsoft, Metacrawler, Altavista]
    - Government's reliance on COTS products and COTS App Dev Environments and the 'maxim' of no single vendor dependency

What is the Problem? - 2

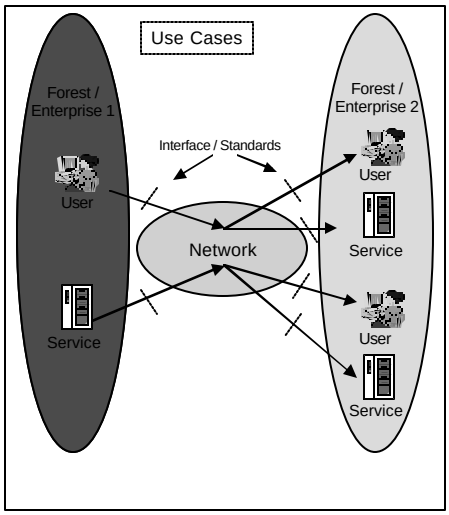
- Distributed systems
  - A single solution even if it were a universally accepted standard will not suffice
    - POSIX, Linux
  - Even within standards there are multiple options that need to be met
    - Profiling is inadequate
    - Dynamic 'Negotiation' is needed
  - Peripheral IA aspects
    - Systems running in more hostile environments
    - Systems being subjected to more systematic attacks
  - Conclusion ➔ Dramatically more complex
- Need to develop new understanding on how to architect, engineer, manage, and operate.
  - Multi Enterprise-Level distributed systems with heterogeneity and diversity using "Federation"

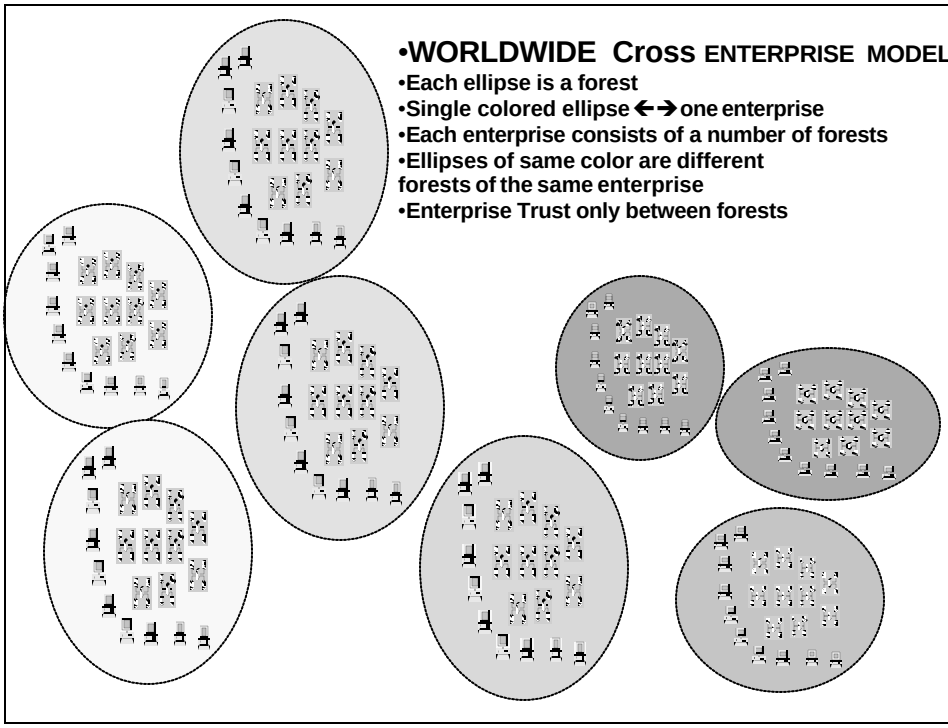
What is Federation?

- What is federation?
  - A **federation** (Latin: *foedus*, covenant) is a union comprised of a number of partially self-governing states or regions united by a central ("federal") government. In a federation, the self-governing status of the component states are typically constitutionally entrenched and may not be altered by a unilateral decision of the central government.
    - European Banking Federation, EU
  - Application to 'computing capabilities'
    - WS-Federation (from BEA, IBM, Microsoft, RSA Security, and Verisign, July 2003) "defines mechanisms that are used to enable identity, account, attribute, authentication, and authorization federation across different trust realms
    - The mechanisms can be used by passive and active requestors; the Web service requestors are assumed to understand the new security mechanisms and be capable of interacting with Web service providers
    - Ability to integrate in a smooth fashion diverse and heterogeneous but similar capabilities
      - Contributing to ease of use for naïve, power and expert users
      - Contributing to less complexity in applications
      - Add complexity to administrators and admin. programs

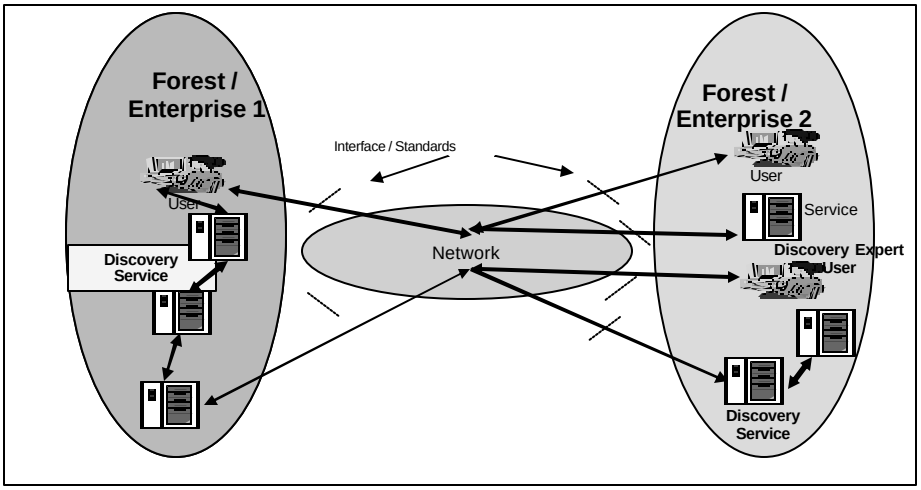
Fundamental Netcentricity Paradigm

- SOA ➔ all interactions via 'services'
  - Everything modeled as a Service
- Netcentricity ➔
  - Any Consumer to Any Provider
    - User – User or Service
    - Service – User or Service
- Interactions enterprise wide or cross enterprise
- Basic interaction paradigm
  - Discover
  - Select and Locate
  - Negotiate
  - Connect
  - Authenticate
  - Access





Enterprise Interaction Complexity



Layered Architecture [Large Grain]

Layering mandatory to address complexity

[Web] Services Higher Layer

[Web] Services Middle Layer

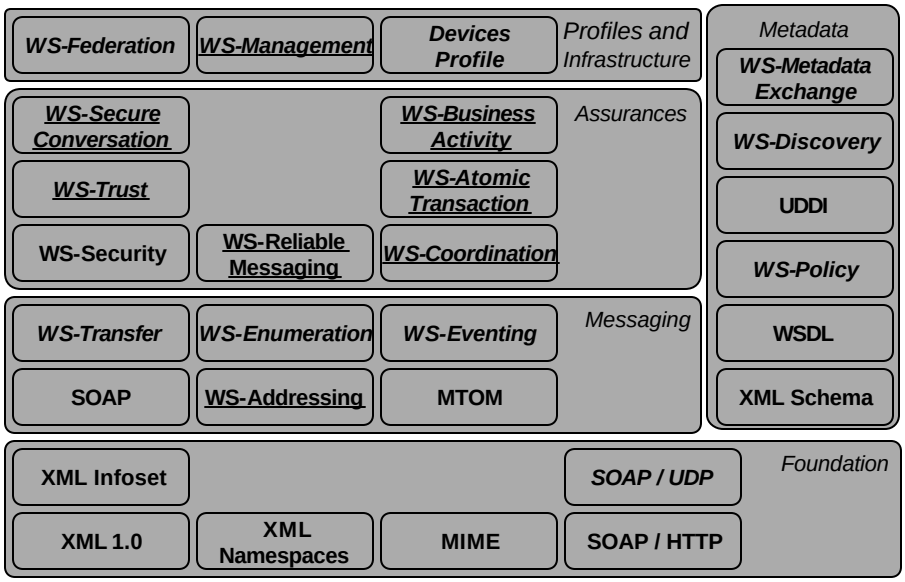
Traditional Middleware
Corba or Pre web services

[Web] Services Lowest Layer

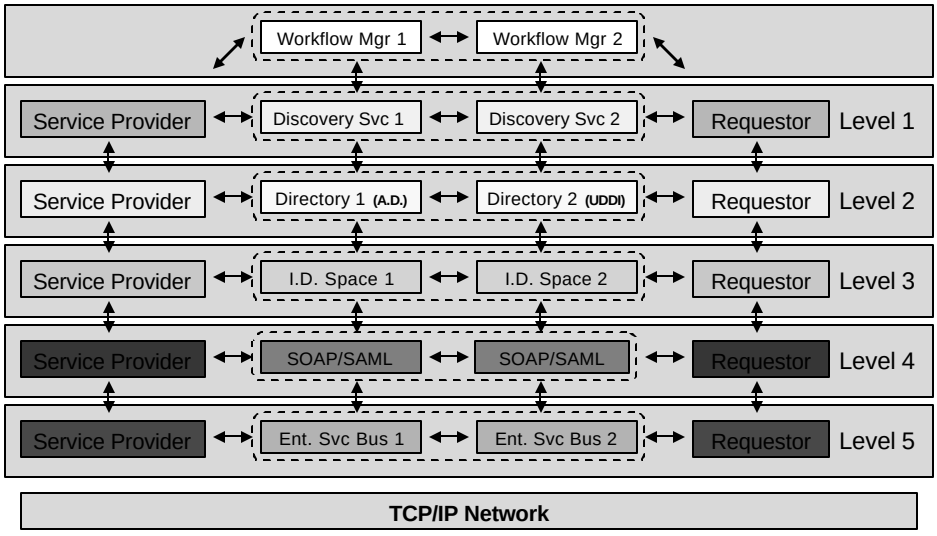
Web Server Service Provider 1	Data Base Mail etc. SP2	Security SP3	Directory SP4	App Server SP ..n	Dist System Capabilities

Distributed OS [Requestor or Provider], Dist Files, Networking protocol stack
Local system management [health, performance, config.], collaboration, messaging
Local security, crypto / certificate, time services

OASIS WS-* Layering



Layering in 'Run time' stack and Federation



Conceptual Model for Federation

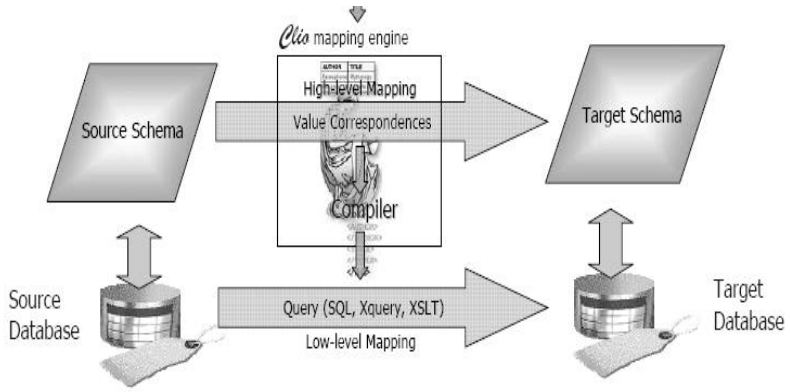
Is there a single model for Federation

- Highly unlikely
- Different models will be needed for
  - Directory Federation [AD, UDDI, Relational Data Base]
  - Identity Federation
    - Identity Space Integration, ID attributes,
  - SAML / Soap
    - Middleware specific messaging
  - Enterprise Service Buses
  - Name spaces, Cross enterprise Bridging
  - Underlying TCP / IP Networking

Data Transparency and Federation

Data Transparency-- Schema Mapping

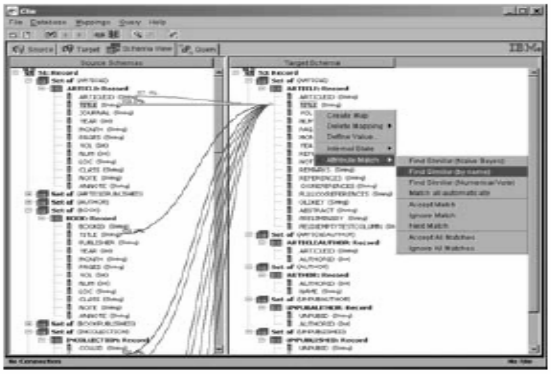
- IBM Tool for mapping across schemas



Data Transparency - Attribute Mapping

Attribute Matcher

The *attribute-matcher* component automatically suggests likely mappings by analyzing the schemas and the underlying data. Our Naïve-Bayes-based matching algorithm has very high success rates, helping the user discover unfamiliar source schemata.



Data Transparency – Query Transformation

- Query Transformation IBM Tool

Transformation Query

Depending on the source type, Clio generates **SQL** queries, or **XQuery** and **XSLT** transformation queries. These queries:

- ✓Produce appropriate grouping
- ✓ Generate Ids where necessary
- ✓ Produce proper target nesting

Directories Identities and Attribute Federation

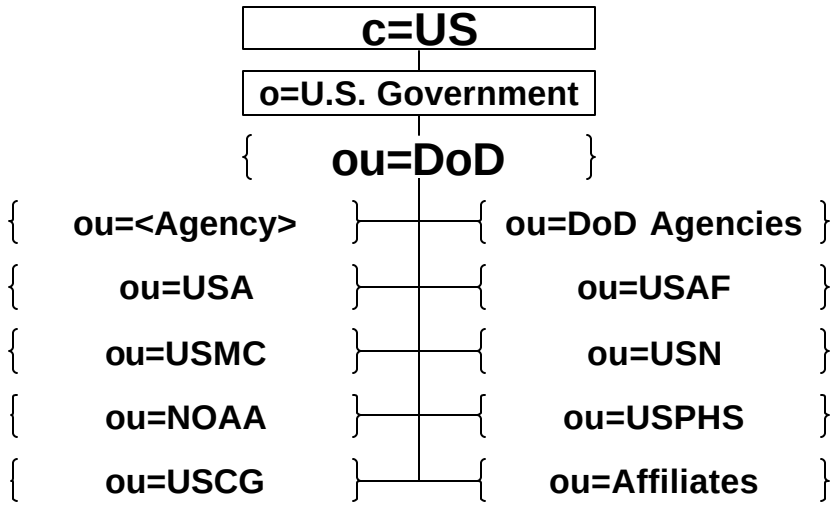
Directories Background

- Directory types considered for use are LDAP and x.500
  - Based on RFCs
  - inetOrgPerson object class used for people
  - Based on commercial requirements
- Active Directory
  - User object class used for people
  - AD User object has inetOrgPerson attributes
- DADIWG AD schema guidance for:
  - Global address list attributes (people)
- DMS provides x.500 schema guidance
  - x.500 not included here

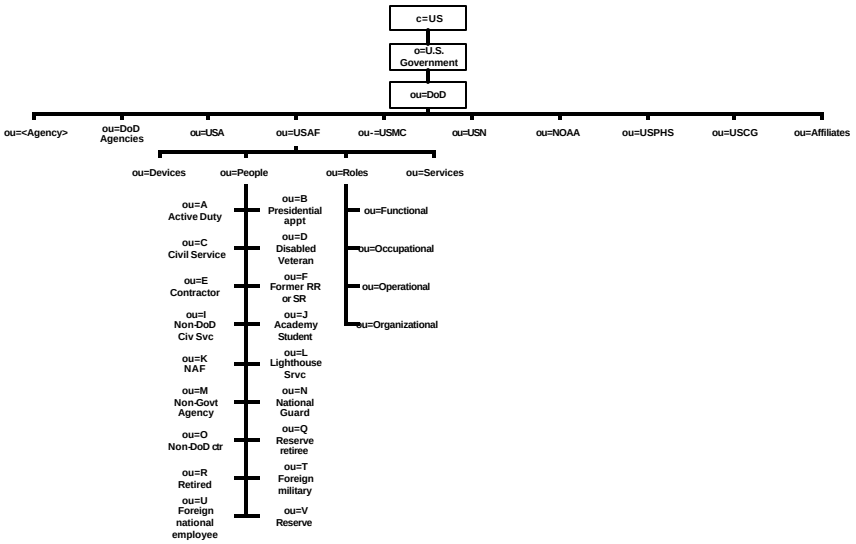
Directory Scope and what it will do

- Capabilities
  - The objective is to implement a standard directory schema in accordance with DoDD 8100.1 that implicitly mandates the use of the Lightweight Directory Access Protocol (LDAP) for digital identities, resulting in a more efficient identity related data synchronization communications for the Air Force and Joint environment.
- Directory ought to address
  - Directory Information Tree (DIT) structure
  - People
  - Roles
  - Devices
  - Services [Middleware and application specific]
  - Object class and attribute naming conventions
- Directory operations need to support:
    - Garrison
    - Tactical
    - Federation with external organizations
  - LDAP and AD instantiations
  - UDDI

Directory Information Tree (1 of 2)



Directory Information Tree (2 of 2)



LDAP People Schema

- Standard LDAP People Object Class
  - inetOrgPerson represents people who are associated with an organization in some way. It is a structural class and is derived from the organizationalPerson class which is defined in X.521.
- New Object Class
  - dodNetOrgPerson is a auxiliary object class that is intended to hold attributes about people in or associated with the Department of Defense.
  - Derived from inetOrgPerson

Active Directory People Schema

- User People Object Class
  - User represents people who are associated with an organization in some way. It is a structural class and is derived from the organizationalPerson class which is defined in X.521.
- New Object Class
  - dodUserOrgPerson is a auxiliary object class that is intended to hold attributes about people in or associated with the Department of Defense.
  - Derived from inetOrgPerson

Unique Identifier for People

- Attribute Name
  - gigID
  - Global Information Grid Identification
- Format
  - The DMDC assigned Electronic Data Interchange Person Identifier appended with the Personnel Category Code
  - [EDI-PI][PCC].
  - Example “0123456789A”.

Directory and Federation Issues

- What directories and when?
  - Do we use lowest common denominator and ignore richness?
  - Where are services and devices registered?
  - Possibly need to separate infrastructure and application spaces
- Naming guidelines and relation to standards
  - DOD Directive [draft] 8130 status?
  - Naming for devices, services, [sensors?]
- What schemas and what are the models for schema mapping?
- What are the models for attribute mapping
  - Common Attributes, Similar and Dissimiliar attributes
  - Domain specific attributes
- Query Transformation across directories and domains
- Who will take it to standards / consortia and get it accepted?
- Scale up, Robustness and other issues

Naming and Federation Issues

- Naming is fundamental to practically everything
- Many different kinds of names being used wout integration
- How does one build federated name spaces?
- Unique Identifiers needed for Services, Systems, Objects, Devices and Containers
  - Must be globally unique
  - Root OIDs issued by ANSI
    - http://www.ansi.org/other_services/registration_programs/reg_org.aspx?me
- ASD Initiative [DOD Draft Directive 8130]
- Common Name
  - [DNS prefix]-[Acronym]-[Description]
  - Example

    af-mil-AIMNT-Connection-Point
- LDAP Display Name
  - [DNS prefix]-[Acronym Description]
  - Example

    afmil-AIMNTConnectionPoint

Authorization and Federation Issues

- What pieces of information will be used for authorization
  - What are the authoritative sources and how will provisioning take place?
  - ABACS helps somewhat but does not solve the problem
  - For ‘groups’ what are the definitions for each forest and where do cross forest or cross enterprise mappings take place?
    - WS-federation does not address these aspects
    - How are group semantics to be matched?
  - How and who will build credentials to contain group information on a per forest and on a per invocation basis?
    - Requestor may select Groups A and B for invocation 1 but only Group B for invocation 2
  - How will revocation work?
  - What will be the relationship between COIs and Groups?
  - Questions similar to the above but now with ‘roles’

Roles

- Roles provide a mechanism to group identities that have a common relationship.
- There are several common relationships that support grouping the types of roles into separate directory branches.
- The intent is to provide a consistent methodology of mapping users under the people branch with roles.
- Role Based Access Control (RBAC) basis for Web Standards (XCAML)
- Standard role schema will support assigning permissions in a more consistent manner between operational directory implementations.

Role Types

Level Six Branch of Military Service, ou=Roles	
ou=Functional	**Consists of a branch for business functions in relationship to mission-applications.**
ou=Occupational	**Consists of a branch for the set of standard job categories that represent competency in a functional area.**
ou=Operational	**Consists of a branch for the job categories associated with operational position or function.**
ou=Organizational	**Consists of a branch for job functions within the context of an organization with some associated semantics regarding the authority and responsibility conferred on individuals assigned to the role.**

Major Issues across all Models

- Who will define solutions and get it accepted across services and 'Joint'?
  - What time frame
  - What is the interim guidance
    - We need things NOW!
- Who will relate the new capabilities to commercially available types?
  - Policy based 'management' may not happen for a long time due to many challenges
- Who will take the new solutions to consortia and standards bodies and get the solutions accepted?
- How and when will we know that other 'ities' are met?
  - Scalability, Dependability, Interoperability …

Way Forward

- Multiple coordinated activities
  - AF, IDA, DISA, selected researchers and a few SMEs will develop and document simple federation models to serve as a start and provide recommendations akin to some level of program guidance for 'programs' in infancy
    - Results in 120 to 150 days
  - IDA, Cornell, Berkeley with OSD /DISA and AFRL support will conduct sustained research and produce more detailed results with feasibility demonstrations based on extensions to vendor capabilities
    - Take results with DISA/ Services to consortia / standards …
    - Duration 24 months [staged results from 12 to 24 months]
- DISA will set up 'drum beat' and plan / organize all major planning activities and make decisions pertaining to governance, candidate selection, usage and acquisition [as needed]
  - DISA will also orchestrate integration of federation capabilities with NCES and NCID

Backups