Towards a Federated SOA Model in Achieving Data Interoperability in DoD

Nick Duan, Ph.D.
ManTech MBI
AFCEA/GMU C4I Symposium
May 20, 2008
Overview

• The Interoperability Challenge and Use of SOA
• Existing SOA Models for Large-Scale, Multi-Organizational Enterprises
  – Centralized Model
  – Fully-Distributed, Peer-to-Peer Model
• The Federated SOA Model
• Achieving Inter-enclave interoperability via federation
• Case Study (Distributed Common Ground System)
• Conclusions
The Interoperability Challenge

• Interoperability as the Key Component in Net-Centric Data Sharing
  – Visibility: Data and Service Discovery, Registry
  – Accessibility: Secure Access, Data Availability Anytime, Anywhere (support of disconnected ops)
  – Understandability: Metadata, Semantic Functions

• Interoperability in a Multi-Organizational Enterprise
  – Different mission focuses
  – Different funding sources
  – Different infrastructure, standards, governance policies
  – Need to balance between structured C2 and autonomy

• Commercial SOA models do not satisfy the needs
Common SOA Models for Implementing Large-scale Enterprises

• Centralized Model
Core services are centralized and difficult to scale and extend, lacks extensibility for the tactical environment

• Fully-Distributed, P2P Model
Lack of governance, discoverability, command and control structure, and the necessary security between service providers and consumers
Alternative: Federation Model

• A typical multi-organizational environment is federated

Model Definition: (Model Structure and Components)
  – a set of loosely coupled, self-contained, individually managed *enclaves*, capable of exchanging data via interacting services by following standard protocols and governance policies, and functioning as independent autonomous units
  – From an network/IA perspective, an enclave is a collection of computing entities interconnected through an internal network and enclosed from the outside network
  – The interface of an enclave to the outside world is usually defined via a single point of presence (POP) (e.g. a web portal)

• Polymorphism of Enclaves
  – An enclave can comprise of multiple sub-enclaves
  – Hierarchical federation structure (for instance, DNS)
The Federated SOA Model

- Implementing the federation model using SOA technologies
- Two basic core services are defined: registry/discovery, security
Inter-enclave Interoperability in a Federation

• Visibility/Discoverability
  – Each enclave is equipped with its own registry and discovery service to allow service registration and discovery at the enclave level

• Accessibility/Access Control
  – Each enclave is responsible for defining and maintaining its own access control policies
  – Enclave POP is the entry point for Inter-enclave accessibility
  – A set of global user roles or attributes are to be established to enable inter-enclave role mapping

• Support of Disconnected Operations
  – Each enclave is able to function as an autonomous unit
Federated Registry

- Federated registry is defined as a set of master/slave registry nodes in a federation hierarchy
- Registry content of a slave is to be replicated on the master via publish-up operations
- Registry content or partial content of a master can be cached on a slave via sync-down operations
Federated Security

• Enterprise identity management solutions may be leveraged for connected operations
  – Establishing trust among enclaves
  – Using SAML/WS-Security to enable cross enclave accessibility

• Access control information of other enclaves is to be cached for disconnected operations
  – User identity and authorization policy info is cached locally within enclaves
  – Standard user roles/attributes are to be established to enable cross domain role mapping
Accessibility in Disconnected Operations

- Step 1: Sync-down user ID and policy info
- Step 2: User access
Case Study of Applying the Federation Model

- Distributed Common Ground System
  - A portfolio of systems to support ISR data processes across multiple DoD Components, Services, and Agencies, including DCGS-AF, DCGS-Army, DCGS-Navy, DCGS-MC, and DCGS-IC
  - Each DCGS member uses different standards and processes for ISR data processing and operations, and has various SOA implementations
  - Interoperability is limited, especially at the tactical level
  - Capability of pushing ISR data to tactical edge is highly desired, as well as support of disconnected operations
The DCGS Federated Enterprise

U.S. Navy Enterprise
U.S. Marine Corps Enterprise
National Reconnaissance Office

DCGS Federated Enterprise Environment

Core Services

U.S. Army Enterprise
U.S. Air Force Enterprise
Other Agencies/Coalition Enterprise
Achieving Interoperability via Federation
Conclusions

• The federated SOA model is a sound and scalable solution in enabling cross-enclave data and service interoperability in a multi-organizational enterprise

• Federated registry and federated security are to be implemented as core services in the federation to support visibility, accessibility and disconnected operations

• Future tasks on improving enterprise federation
  – Governance standards and policies on federation processes and procedures for forming, joining, and leaving a federation
  – Standards and protocols for publish-up and sync-down operations (content-staging in a federated environment)
Q&A